Marie-Luise Shnayien

DIE UNSICHEREN KANÄLE

Negative und queere Sicherheit in Kryptologie und Informatik



[transcript] Digitale Gesellschaft

Marie-Luise Shnayien
Die unsicheren Kanäle

Digitale Gesellschaft | Band 51

Diese Publikation wurde im Rahmen des **Fördervorhabens 16TOA002 mit Mitteln des Bundesministeriums für Bildung und Forschung** sowie mit Mitteln der Open Library Community Medienwissenschaft 2022 im Open Access bereitgestellt.

Die Open Library Community Medienwissenschaft 2022 ist ein Netzwerk wissenschaftlicher Bibliotheken zur Förderung von Open Access in den Sozial- und Geisteswissenschaften:

Vollsponsoren: Humboldt-Universität zu Berlin | Staatsbibliothek zu Berlin – Preußischer Kulturbesitz | Technische Universität Berlin / Universitätsbibliothek | Universitätsbibliothek der Ruhr-Universität Bochum | Universitäts- und Landesbibliothek Bonn | Staats- und Universitätsbibliothek Bremen | Universitäts- und Landesbibliothek Darmstadt | Sächsische Landesbibliothek, Staats- und Universitätsbibliothek Dresden (SLUB Dresden) | Universitätsbibliothek Duisburg-Essen | Universitäts- und Landesbibliothek Düsseldorf | Universitätsbibliothek Johann Christian Senckenberg Frankfurt am Main | Albert-Ludwigs-Universität Freiburg / Universitätsbibliothek | Niedersächsische Staats- und Universitätsbibliothek Göttingen | Universitätsbibliothek der FernUniversität in Hagen | Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek | Karlsruher Institut für Technologie (KIT) – KIT-Bibliothek | Universitätsbibliothek Kassel | Universitätsbibliothek in Landau | Universität zu Köln, Universitäts- und Stadtbibliothek | Universitätsbibliothek Leipzig | Universitätsbibliothek Mannheim | Universitätsbibliothek Marburg | Universitätsbibliothek der Ludwig-Maximilians-Universität München | Fachhochschule Münster | Universitäts- und Landesbibliothek Münster | Bibliotheks- und Informationssystem der Universität Oldenburg | Universitätsbibliothek Siegen | Universitätsbibliothek Vechta | Universitätsbibliothek der Bauhaus-Universität Weimar | Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth | Zürcher Hochschule der Künste | Zentralbibliothek Zürich
Sponsoring Light: Universität der Künste – Universitätsbibliothek | Freie Universität Berlin | Fachhochschule Bielefeld, Hochschulbibliothek | Hochschule für Bildende Künste Braunschweig | Fachhochschule Dortmund, Hochschulbibliothek | Technische Universität Dortmund / Universitätsbibliothek | Bibliothek der Pädagogischen Hochschule Freiburg | Hochschule Hannover – Bibliothek | Landesbibliothek Oldenburg | Akademie der bildenden Künste Wien, Universitätsbibliothek | ZHAW Zürcher Hochschule für Angewandte Wissenschaften, Hochschulbibliothek
Mikrosponsoring: Filmmuseum Düsseldorf | Bibliothek der Theologischen Hochschule Friedensau | Bibliothek der Hochschule für Musik und Theater Hamburg | Hochschule Hamm-Lippstadt | Bibliothek der Hochschule für Musik, Theater und Medien Hannover | ZKM Zentrum für Kunst und Medien Karlsruhe Bibliothek | Hochschule Fresenius | Filmuniversität Babelsberg KONRAD WOLF – Universitätsbibliothek | Bibliothek der Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt (FHWS)

Marie-Luise Shnayien

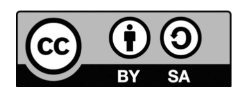
Die unsicheren Kanäle

Negative und queere Sicherheit in Kryptologie und Informatik

[transcript]

Die erste Fassung der vorliegenden Publikation ist 2021 von der Fakultät für Philologie an der Ruhr-Universität Bochum als Dissertation angenommen worden. Gutachterinnen: Prof. Dr. Anna Tuschling, Prof. Dr. Astrid Deuber-Mankowsky, Datum der Disputation: 01.07.2021
Diese Publikation wurde im Rahmen des Fördervorhabens 16TOA002 mit Mitteln des Bundesministeriums für Bildung und Forschung im Open Access bereitgestellt.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.



Erschienen 2022 im transcript Verlag, Bielefeld

Umschlaggestaltung: Maria Arndt, Bielefeld
Korrektorat: Len Klapdor
Druck: Majuskel Medienproduktion GmbH, Wetzlar
https://doi.org/10.14361/9783839463062
Print-ISBN 978-3-8376-6306-8
PDF-ISBN 978-3-8394-6306-2
EPUB-ISBN 978-3-7328-6306-8
Buchreihen-ISSN: 2702-8852
Buchreihen-eISSN: 2702-8860

Inhalt

1. Einleitung

»For thus all things must begin, with an act of love.« *(Marais in Haraway 1997, 123)*

Mit diesen Worten des südafrikanischen Naturforschers Eugene Marais beginnt Donna Haraways Essay *enlightenment@science_wars.com: A Personal Reflection on Love and War.* Und auch dieses Buch, in dem die Verflechtungen von Kryptologie, IT-Sicherheit und Geschlecht im Hinblick auf Fragen nach Sicherheit aus gender-medienwissenschaftlicher Perspektive untersucht werden, ist, zumindest in Teilen, ein persönliches Nachdenken über Liebe und Krieg zwischen verschiedenen Fachkulturen. Nicht zuletzt, da das vorliegende Buch zu großen Teilen in einem sehr prägenden Umfeld entstanden ist: dem interdisziplinären NRW-Forschungskolleg *SecHuman – Sicherheit für Menschen im Cyberspace,* dessen Teil ich von Anfang 2017 bis Mitte 2020 sein durfte, und dessen Forschungszusammenhänge über dieses Zeitfenster hinaus bestehen geblieben sind. Im Kern von *SecHuman* stand ein starker Interdisziplinaritätsanspruch: Aufgeteilt in 6 Themenbereiche, jeweils paritätisch besetzt mit einem_einer Doktorand_in aus den Bereichen Jura, Geistes- oder Sozialwissenschaft, sowie einem_einer Doktorand_in aus einem mathematisch-technischen Fach, und von einer weiteren Promotion begleitet, die die Wissensintegration in den jeweiligen ›Promotionstandems‹ untersuchen sollte. Ziel dieser Konstellation war, dass diese ›Promotionstandems‹ sich gegenseitig inspirieren, sowie fachlich ergänzen und so in einem interdisziplinären Austausch in Bezug auf die jeweiligen Themenschwerpunkte tiefergehendes Wissen produzieren würden als eine jeweilige Disziplin allein dies könnte. Eine solche Aufteilung setzt ein komplexeres Verständnis von Phänomenen digitaler Kulturen voraus, und erkennt an, dass Phänomene nicht aus jeweils nur einer Sichtweise heraus ausreichend erfasst werden können, bringt

jedoch auch spezifische Hürden mit sich. Interdisziplinäres Forschen ist bereits unter Fächern, die derselben Fakultät angehören, nicht leicht, und über die Grenzen der eigenen Fakultät hinaus ist es nicht nur aufgrund der unterschiedlichen Erkenntnisinteressen und Methoden der jeweiligen Fächer ein schwieriges Unterfangen, sondern auch aufgrund der belasteten Vorgeschichte des Verhältnisses von Natur- und Geisteswissenschaften, die in der jüngeren Geschichte vor allem in den sogenannten *Science Wars* sichtbar wurde, auf die ich an dieser Stelle daher kurz eingehen möchte.

Als *Science Wars* wird eine Auseinandersetzung bezeichnet, die vornehmlich in den 1990er Jahren in den USA ausgetragen wurde. Als auslösendes Ereignis lässt sich mit Martin Doll (2012, 276) die Entscheidung des US-Kongress begreifen, im Jahr 1993, zum ersten Mal seit Ende des Zweiten Weltkriegs, keine Gelder für naturwissenschaftliche Forschung bereitzustellen, weshalb ein beantragter Teilchenbeschleuniger nicht finanziert wurde. Renommierte Naturwissenschaftler_innen machten daraufhin die *Science Studies*, also die Wissenschaftsforschung, sowie den von ihnen in dieser Forschung vermuteten Relativismus für diese Entscheidung verantwortlich. Ein Jahr später erschien das Buch *Higher Superstition: The Academic Left and Its Quarrels With Science* von Paul Gross und Norman Levitt (vgl. ebd.). Wie Martin Doll (ebd.) ausführt, warfen Gross und Levitt den Geistes- und Sozialwissenschaften vor, eine »die Errungenschaften der Aufklärung zunichtemachende Haltung« einzunehmen, indem einzelne Wissenschaftler_innen sich »zwar selbst in die Tradition linker Kritik« einreihten, aber schlussendlich politisch wirkungslos blieben. Treibende Konzepte dieser Bewegung seien dabei Marxismus, Postmodernismus, Feminismus, Konstruktivismus sowie Multikulturalismus (vgl. ebd.). Einen diskursiven Höhepunkt erreichten die *Science Wars* zwei Jahre später mit dem sogenannten *Sokal-Hoax*: der Veröffentlichung eines Artikels des US-amerikanischen Physikers Alan Sokal mit dem Titel *Transgressing the Boundaries: Towards a Transformative Hermeneutics of Quantum Gravity* in einer Ausgabe des sozialwissenschaftlichen Journals *Social Text*, die sich schwerpunktmäßig mit den *Science Wars* befasste (vgl. Sokal 1996b). Nur drei Wochen später veröffentlichte Sokal einen weiteren Artikel im Journal *Lingua Franca*, in dem er *Transgressing the Boundaries* als wissenschaftliche Fälschung enttarnte: Dem Artikel liege eine komplett unwissenschaftliche Argumentation zugrunde, was für »any competent physicist or mathematician (or undergraduate physics or math major)« (Sokal 1996a) leicht zu erkennen sei. Den Herausgeber_innen von *Social Text* warf Sokal vor, niemanden für die Evaluierung seines Artikels zu Rate gezogen zu haben, der_die diesen hätte einschätzen können,

und kommt damit zu dem Schluss, dass die Herausgeber_innen interessierter an den in seinem Text artikulierten politischen Forderungen gewesen seien als an *tatsächlichen* wissenschaftlichen Erkenntnissen (vgl. ebd.). Eine Kritik, die Doll (2012, 282) vorsichtig teilt, wobei er kritisch anmerkt, dass die nach nur drei Wochen erfolgte Enttarnung des Fakes nichts darüber aussage, wie der Hoax-Artikel von anderen Wissenschaftler_innen innerhalb der Community aufgenommen worden wäre, und ob es nicht auch kritische Besprechungen hätte geben können (vgl. ebd., 285), die die bis dahin bereits formulierten Anschuldigungen gegen die Geistes- und Sozialwissenschaften außer Kraft gesetzt hätten. Stattdessen folgte auf den Sokal-Hoax, wie Haraway (1997, 123) es ausdrückt, »a neverending profusion of pungent comment, complaint, exultation, accusation, and analysis on all sides« – eine Gemengelage, die, wie Doll (2012, 280–281) deutlich macht, auch durch die stark verkürzte und skandalisierende mediale Aufarbeitung in Tagespresse, Fernsehen und Radio begünstigt wurde. Im Zuge der durch die Berichterstattung vorgenommenen argumentativen Verflachungen ergriff Doll zufolge auch ein nicht unerheblicher Teil der berichtenden Medien Partei für Sokal: Doll (ebd.) konstatiert, dass sich »das vorherrschende undifferenzierte Bild, das die Massenmedien zeichneten, als allgemeine Diskreditierung von geistes- und sozialwissenschaftlichen Infragestellungen unveränderlicher Wahrheiten oder Fakten sowie der Erkenntnispraktiken, die ihr Zustandekommen regeln,« beschreiben lässt, was schließlich, wie Haraway (1997, 128) es formuliert, in einem »commercialized and rigged epistemological Super Bowl where the only teams on the globe are *Realism* and *Relativism*« mündete. Zugespitzt formuliert, ereignete sich in den *Science Wars*, befeuert durch Unzufriedenheit über Förderungspolitiken, eine Kollision naturwissenschaftlich-empirischer Methoden mit den in den Geisteswissenschaften an Bedeutung gewinnenden theoretischen und methodischen Erkenntnissen der Postmoderne und des Poststrukturalismus. Mit dieser Kollision verbindet sich gleichsam ein Schlag der Naturwissenschaften gegen die Geisteswissenschaften, und insbesondere auch gegen die Wissenschaftsforschung, der sich als ein methodischer Streit um die Formen der Wissensproduktion und um den Status von Faktizität und Wissen beschreiben lässt.

Warum dieses Buch direkt mit einem Hinweis auf diesen so verbittert ausgetragenen Streit zwischen Disziplinen beginnen, der nun auch bereits fast 25 Jahre alt ist? Da die von Haraway (ebd., 123) beschriebenen »accusations brought by Sokal, Gross, Levitt, and their allies, that there are dubious folks among us, called by the ominous-sounding name of ›constructionists,‹

who ›do not believe in reality,‹ or at least not in science, enlightenment, and facts« auch mir begegnet sind, obwohl meine Position eine andere ist als die Haraways und ihrer Kolleg_innen. Dies geschah, mal mehr und mal weniger explizit, besonders zu Beginn meiner Zeit bei *SecHuman* in der Form von Misstrauen gegenüber meinem methodischen Vorgehen, sowie einer Ablehnung meiner Forschungsergebnisse und deren Konsequenzen, und war nicht leicht zu navigieren.[1] Dennoch liegt in dieser Kontextualisierung meinerseits keine Anschuldigung, keine Verbitterung, und auch kein Wunsch, die *Science Wars* fortzuführen oder den initialen Konflikt zu lösen – vielmehr ist es eine Beobachtung, die zur Situierung und damit zum Verständnis dieses Buchs und seiner Eigenheiten hilfreich ist, sowie der Versuch, die Politiken der Versöhnung, der disziplinären Annäherungen, die sich nach und nach im Kontext des Forschungskollegs eingestellt haben, und zu denen auch die vorliegende Untersuchung beiträgt, genauer in den Blick zu nehmen.

1.1 Attachments und die Frage nach der eigenen Methode

Meine Zeit bei *SecHuman* war allen Schwierigkeiten zum Trotz gekennzeichnet von einer überaus produktiven Zusammenarbeit, wie sie in den letzten Jahren vor allem im Zuge einer an Phänomenen digitaler Kulturen interessierten Medienwissenschaft eingefordert wurde: Der Austausch zwischen meinem Tandempartner Benedikt Auerbach und mir über Kryptologie und die Frage, was Sicherheit bedeutet, war nicht frei von methodischen Konflikten, aber auch gezeichnet von einer »intellectual generosity or curiosity toward those whose practices are not our own«, die mit Tara McPherson (2012, 36) als Voraussetzung für das Forschen zu, aber auch mit und in digitalen Kulturen verstanden werden kann. Rückblickend kann ich sagen, dass ich durch *SecHuman* trotz, aber auch gerade aufgrund der disziplinären und methodischen Uneinigkeiten und Auseinandersetzungen viel von meinen Kolleg_innen und den beteiligten Professor_innen gelernt habe, und diesem Austausch sehr verpflichtet bin. Die mir ermöglichten Einblicke in andere Fachkulturen stellen eine der Voraussetzungen für die in diesem Buch festgehaltenen Ergebnisse dar: Ich

1 Christoph Engemann, Till Heilmann und Florian Sprenger (2019, 155) ist insofern Recht zu geben, wenn sie bemerken, Methoden (und die Frage nach der Methode) seien ein Mittel der Disziplinierung.

durfte, mit Donna Haraway (1997, 124) gesprochen, ein tieferes Verständnis dafür entwickeln,

> »that knowledge is always an engaged material practice and never a disembodied set of ideas. Knowledge is embedded in projects; knowledge is always for (in many senses of for) some things and not others, and knowers are always themselves formed by their projects, just as they shape what they can know.«

Diese Situierung von Forscher_innen und ihren Wissensobjekten, die Haraway hier beschreibt, möchte ich im Folgenden mit Isabel Stengers (2005) als *Attachment* begreifen. In ihrem Aufsatz *Introductory Notes on an Ecology of Practice* greift Stengers (ebd., 191) den Begriff des Attachments von Bruno Latour auf, und schreibt: »Attachments are what cause people, including all of us, to feel and think, to be able or to become able.« Das Attachment ist für Stengers (ebd.) verbunden mit einer Form von Zugehörigkeit (*belonging*), und darf nicht mit einer Verpflichtung (*obligation*) verwechselt werden, von der man sich befreien könnte. Bezugnehmend auf das Denken in wissenschaftlichen Zusammenhängen schreibt sie weiter:

> »We may well present ourselves as free, detached of superstitious beliefs, able to enter long networks, but the moment you try to tell physicists that their electrons are only a social construction, you will get war. And you will have deserved it because you have insulted not simply their beliefs but what attaches them, causes them to think and create in their own demanding and inventive way.« (Ebd.)

Ein *Attachment* ist also, was einen ins Denken bringt, und kann weiterhin mit Haraway als Form der Anhänglichkeit verstanden werden, als eine liebevolle Haltung, die nicht nur Haraway gegenüber der von ihr untersuchten Biologie einnimmt, sondern die auch die von ihr betrachteten Forscher_innen gegenüber ihren Gegenständen einnehmen. Dies bedeutet nicht, dass die Forscher_innen ihren Gegenständen nur positive Gefühle entgegenbrächten, sondern bezieht sich vielmehr auf die von Stengers beschriebene Form der Zugehörigkeit, auf ein Zuhause-Sein in den Theorien und bei den Gegenständen, die einen ins Denken bringen, in der sie beschreibenden Sprache und der eigenen Form der Wissens- und Sinnproduktion. Auch *SecHuman* war ein Knotenpunkt unterschiedlichster Fachkulturen, in dem die Doktorand_innen und Professor_innen mit ihren jeweiligen Attachments, Einsätzen und Methoden verbundenes Wissen produziert haben, die gleichsam auch

geformt haben, was die jeweiligen Disziplinen überhaupt wissen können. Dieses Umfeld hat von allen Beteiligten eine Form der Flexibilität verlangt, ein Sich-Einlassen auf diese verschiedenen Formen der Wissensproduktion der jeweiligen Disziplinen, aber auch ein Vermitteln der eigenen Arbeitsweise für eine grundsätzlich fachfremde Zuhörer_innenschaft. Für die von mir angestrebte medienwissenschaftliche Arbeit über die Wissensgeschichte der IT-Sicherheit hat das bedeutet, mich einerseits sehr auf die innerfachlichen Diskurse der IT-Sicherheit und der Kryptologie einzulassen, aber andererseits auch aufzupassen, nicht komplett in diesen aufzugehen, und die eigenen Betrachtungen den dort vorzufindenden Strukturen unterzuordnen – eine Tendenz, die auch McPherson (2012, 34) beim Verfassen ihres Texts, der die Gemeinsamkeiten der Funktionsweisen von UNIX-Programmierung und Rassismus verhandelt, bemerkt hat. Es geht ein ganz eigener Sog von mathematisch-technischer Wissensproduktion aus: von Formeln, Funktionen und Funktionalitäten, Studien, Statistiken, scheinbar greifbareren Ergebnissen – und als eine der wenigen nicht empirisch forschenden Promovend_innen im Kontext von *SecHuman* war dieses Spannungsfeld der Methodenvielfalt in manchen Momenten mit einem Rechtfertigungsdruck verbunden, denn, wie Anna Tuschling (2020, 177) in ihrem Artikel *Methoden sind politisch*[2] formuliert, »für viele Wissenschaften hängt ihr Wissenschaftsverständnis – und in ihren Augen damit Wissenschaftlichkeit als solche – an der Kenntnis und Passung der genutzten Methoden.« Tuschling (ebd.) weist weiter darauf hin, dass es zwar selbstverständlich keine Wissenschaft ohne Methode gebe, aber dass es durchaus stärker empirisch arbeitende Disziplinen gebe, zu denen »die Medienwissenschaft bislang aufgrund ihrer eigenen Methoden, Ansätze und Theorien mit guten Gründen allenfalls in Teilen« gehöre. Empirische Methoden, konstatiert Tuschling, fänden derzeit vor allem im Kontext von und unter Bedingungen von Digitalität Anwendung, die durch eine Fülle digitaler Daten gekennzeichnet seien. Dennoch böten diese Kontexte »eine große Chance gerade für die nicht quantitative, kritische Erforschung digitaler Umgebungen«, wobei das Potential einer qualitativen medienwissenschaftlichen Forschung vor allem darin liege, »ihren Umgang mit den wissenschaftlichen Methoden

2 Ungefähr zeitgleich mit der Arbeit an diesem Buch ist auch innerhalb der deutschsprachigen Medienwissenschaft ein produktiver Streit darum entbrannt, was eigentlich medienwissenschaftliche Methoden sind und leisten sollen. Siehe dazu exemplarisch Schüttpelz (2019), Sprenger et al. (2020), Vonderau (2019), sowie den stetig aktualisierten *Open Media Studies Blog*.

im engeren Sinne selbstbestimmt und kritisch zu gestalten.« (Ebd.) Im Folgenden möchte ich daher die Eckpfeiler meines methodischen Vorgehens skizzieren.

1.2 Wie medienwissenschaftlich über Technik schreiben?

Das Projekt dieses Buchs ist eine wissensgeschichtliche Analyse der Konzeptionierung von Sicherheit in Kryptologie und Informatik, sowie eine Exploration der Anschlussstellen dieser Geschichte an Fragen nach Geschlecht und Körperlichkeit, an deren Ende ein Nachdenken über einen alternativen Sicherheitsbegriff steht. Die methodische Grundlage meiner Untersuchung bildet Michel Foucaults Diskursanalyse. Eine solche Diskursanalyse fragt danach, was zu einem bestimmten Gegenstand geäußert wird, aber auch, wie, wann und unter welchen Umständen, zu welchem Preis es geäußert wird sowie danach, was nicht geäußert wird oder werden kann. Mit Foucaults Konzept der *Problematisierung* (vgl. exemplarisch Foucault 1996, 178–179) geht es mir dabei um die Frage, warum und zu welchen Bedingungen Wissen über einen Gegenstand, in diesem Fall: IT-Sicherheit, produziert wird und wie dieser Gegenstand damit überhaupt erst entstanden ist. Obgleich diese Herangehensweise plausibel erscheinen mag, ist die Legitimation der Verwendung von Diskursanalyse für eine medienwissenschaftliche Analyse digitaler Medien nicht unumstritten. Markus Stauff (2005, 126) weist in seinem Aufsatz *Mediengeschichte und Diskursanalyse. Methodologische Variationen und Konfliktlinien* darauf hin, dass sich die Foucault'sche Diskursanalyse »als wissenschaftshistorische Methode« nutzen lässt, »die es ermöglicht, die Konstitution des historischen und kontingenten Gegenstands ›Medien‹ und die Möglichkeitsbedingungen eines Wissens von den Medien nachzuvollziehen«, wobei die Stärke dieser Herangehensweise darin liege, die

> »Gegenstände – also auch ›die Medien‹ – nicht vorauszusetzen und nicht vor der Analyse zu definieren, sondern ihre ereignis- und wechselhafte, sehr wohl aber ›reale‹ Hervorbringung in den historisch vorliegenden Diskursen und Praktiken zu rekonstruieren.«

Dennoch werde der diskursanalytischen Medienwissenschaft vor allem seitens der »technikorientierte[n] Mediengeschichtsschreibung« innerhalb der deutschsprachigen Medienwissenschaft eine Technik- und Ökonomievergessenheit vorgeworfen (vgl. ebd.). Stauff bezieht sich hier vor allem auf eine

technikorientierte Mediengeschichtsschreibung in der Tradition Friedrich Kittlers, die der Foucault'schen Diskursanalyse eine unzureichende Kraft für die Analyse gerade digitaler Medien attestiere, da diese Methode »blind für die Hardware und die alle Sinne unterlaufenden Effekte technischer Medien« (ebd., 127) bliebe. Damit wird das in Kittlers pointiertem (und wohl meistzitiertem) Diktum »Medien bestimmen unsere Lage« (Kittler 1986, 3) enthaltene medientechnische Apriori in Stauffs Lesart zu einem unüberwindbaren Hindernis für die Diskursanalyse, da es in dieser Logik immer etwas gibt, was dem Diskurs vorgängig bleibt, diesen quasi vor*formatiere* – und sich damit als Möglichkeitsbedingung des Denkens demselben über eine Diskursanalyse auch stets entziehe. Doch was für ein Diskursbegriff liegt dieser Kritik zugrunde? Interessanter Weise, so bemerkt Stauff (2005, 128), verwende Kittler in *Grammophon, Film, Typewriter* Diskursanalyse, um auf genau diesen »Bereich des eigentlich Medialen« aufmerksam zu machen, »der von der Diskursanalyse nicht erfasst werden könne.« In dieser Tradition verortet Stauff auch Wolfgang Ernsts (2000, 20) Aussage, dass eine »wohldefinierte Medienwissenschaft […] es mit den Ereignissen und Geheimnissen des Non-Diskursiven zu tun« habe. Stauff (2005, 131–132) folgend handelt es sich bei diesem Diskursbegriff jedoch um eine Art Schwundstufe der Foucault'schen Diskursanalyse, die lediglich Diskurse *über* Medien, nicht aber die Medien selbst analytisch fassen könne. Während ich durchaus der Forderung nach einer technischen Kompetenz der Medienwissenschaft[3] als grundlegende Notwendigkeit für die Analyse digitaler Phänomene zustimme, und auch durch *SecHuman* im kleineren Rahmen eine formale Ausbildung in Grundlagen der Kryptographie und IT-Sicherheit genossen habe, was in der vorliegenden Untersuchung sichtbar wird,[4] so möchte ich doch mit Markus Stauff für einen weiteren Diskursbegriff plädieren, der das Technische miteinschließt, denn: Die Stärke der Diskursanalyse als medienwissenschaftlicher Methode liegt im bereits genannten Vorgang der *Problematisierung*, der es ermöglicht, die

3 Diese Forderung wird heute vor allem von Wolfgang Ernst (2018; 2000) sowie von Stefan Höltgen (2020; 2019; 2018) vertreten, allerdings einhergehend mit der Behauptung, dass Fragen nach dem Performativen sowie nach Körpern, und damit auch nach Geschlecht nicht in das Feld der Medienwissenschaft fielen. Die vorliegende Untersuchung wendet sich sowohl methodisch als auch inhaltlich gegen diese Behauptung, sowie gegen die von Ernst proklamierte »wohldefinierte Medienwissenschaft« (Ernst 2018, 20), die er auch als »Mediamatik« (ebd., 11) bezeichnet.

4 Um eine Lektüre ohne technische Vorkenntnisse zu ermöglichen, werden alle für das Verständnis der Argumentation zentralen technische Begriffe und Konzepte erläutert.

fokussierten Objekte nicht als bereits gegeben zu betrachten. Dies versetzt eine diskursanalytische Mediengeschichte in die Lage, Medien grundsätzlich als »in keiner Phase ihrer historischen Existenz stabile, den Diskursen und Praktiken entzogene Konstellationen« (ebd., 133) zu begreifen, und sie somit nicht nur zum Zeitpunkt ihrer Entstehung, an ihren Bruchstellen oder Störungen in den Blick zu bekommen. Ein umfassender Eindruck von Medien entstehe Stauff (ebd.) zufolge »nur dort, wo bestimmte technische, inhaltliche, rezeptive sowie medienpolitische Varianten zu einer dynamischen, umstrittenen und deshalb produktiven Konstellation gebündelt« werden. Er konstatiert weiter:

> »In der Folge können eben auch Technologien als Diskurse [...] verstanden werden. Dies heißt nicht, dass [...] mediale oder technische Effekte nur auf der Ebene der Diskurse zu suchen wären. Es zielt lediglich darauf, ›Diskurse als ebenso konstitutiven Teil der Wirksamkeit einer Technologie‹ zu betrachten ›wie die in Laboren, Universitäten, Werkstätten und Garagen entwickelte Hardware‹. Diskursivierungen versehen Medien mit Definitionen und Differenzierungen, die sich nicht von den Apparaten oder den ›Inhalten‹ ableiten lassen, aber in Ankopplung an diese die Medien handhabbar machen und mit spezifischen Rationalitäten versehen.« (Ebd.)

Um seinen Standpunkt zu stärken, führt Stauff (ebd.) das Beispiel eines Ingenieurs an, für den es nicht *das* Fernsehen gebe, sondern »immer schon ein durch konkurrierende Diskursivierungen geprägtes Fernsehen, das seinen Strategien bestimmte Zugriffspunkte bietet.« Dieses Verständnis der Interaktion von Technik und Diskursen macht deutlich, dass auch Technik nicht außerhalb von Diskursen steht, und bietet ebenfalls einen Anschlusspunkt an das mit Haraway und Stengers beschriebene *Attachment* von Forschenden zu ihren Methoden und Gegenständen, das alle drei situiert, sowie den Rahmen, also die Möglichkeitsbedingungen der Wissensproduktion bestimmt. Stauff (ebd.) resümiert nach einigen Beispielen: »Gerade weil diese Untersuchungen kein vorgängiges Medium annehmen, können sie verdeutlichen, wie Diskurse Verflechtungen mit Praktiken und Apparaten eingehen, die die Diskurse stützen und zugleich durch sie Wirksamkeit erhalten.« Doch das Denken *von* und das Schreiben *über* Technik, sofern man diese als nicht außerhalb von Diskursen oder als diesen vorgängig auffasst, birgt eine weitere Schwierigkeit.

1.3 Ungehörige Übertragungen

Abgesehen von der banalen Feststellung, dass es zu den eigenen Forschungsgegenständen zusätzlich zum *Attachment* auch eine gewisse Distanz braucht, um diese kritisch befragen zu können, soll an dieser Stelle noch ein spezifischer Aspekt des Technischen, nämlich die von Tara McPherson beobachtete Sogwirkung desselben, aber auch die der *hard sciences*, besprochen werden. »So if we are always already complicit with the machine, what are we to do?«, fragt McPherson (2012, 34) und leitet so ihre Beobachtung ein, dass der Computer, *an* dem und *über* den sie schreibt, ihr Schreiben mitgestaltet. Sie beschreibt, dass sie sich selbst dabei ertappt, wie die Funktionalität des Computers, »the logic of modularity« (ebd.), und die damit einhergehende Aufteilung der Welt in Wissensbereiche, die miteinander scheinbar nichts zu tun haben, beständig Einfluss auf ihr Schreiben nimmt. McPherson verbindet diesen Eindruck jedoch nicht mit dem Verweis auf ein technisch Unbewusstes oder ein medientechnisches Apriori, sondern politisiert ihn durch ihre Lesart als einen Mangel an Wissen der geisteswissenschaftlich Forschenden gegenüber ihren digitalen Gegenständen. McPherson (ebd., 34–35) schreibt weiter, dass die oft gestellten Fragen nach Repräsentation und Narration, und etwas allgemeiner der »very intense focus on visuality«, den sie innerhalb der geisteswissenschaftlichen Forschung der letzten 20 Jahre ausmacht, zu der sie auch ihre eigenen Arbeiten zählt, als ein Symptom dieser Logik der Modularisierung und als »a distraction from the powers that be« gelesen werden könnten. Ohne diese Zuspitzung in voller Härte zu teilen, entfaltet die vorliegende Untersuchung ihre Überlegungen dennoch hauptsächlich anhand der inneren Beschaffenheit von kryptographischen Verfahren und IT-Systemen, und befasst sich nur selten mit Fragen nach Repräsentation und Visualität. »To push my polemic to its furthest dimensions«, schreibt McPherson (ebd., 35) nach einigen Spitzen weiter, »I would argue that to study image, narrative and visuality will never be enough if we do not engage as well the non-visual dimensions of code and their organization of the world.« Dabei steht einiges auf dem Spiel: McPherson (ebd., 23) begreift die Funktionsweise von UNIX-Systemen und von *racial segregation* in den USA nicht nur als strukturell ähnlich, sondern auch als »mutually reinforcing« – was in letzter Konsequenz bedeutet, dass Technik ebenso in den antirassistischen

Kampf eingebunden sein muss, wie andere Bereiche des Lebens.[5] Aller Kenntnis dieser »non-visual dimensions of code« zum Trotz, so konnte ich beim Schreiben an diesem Buch feststellen, bleibt die Anziehungskraft des Technischen bestehen, und sorgt bisweilen dafür, dass informatische Konzepte sich in die Theoriebildung integrieren möchten. Während eine in der Tradition der »wohldefinierten Medienwissenschaft« (Ernst 2000) stehende Untersuchung dies entsprechend einem medientechnischen Apriori affirmieren würde, was beispielsweise in dem rezenten Vorschlag, eine mathematik- und techniknahe Medienwissenschaft als »Mediamatik« zu bezeichnen (Ernst 2018, 11), sichtbar wird, möchte ich dies weiterführend mit Astrid Deuber-Mankowsky (2020; 2017a) problematisieren. In ihrem Aufsatz *Das ontologische Debakel oder was heißt: Es gibt Medien?* plädiert Deuber-Mankowsky (2017a) für eine medienphilosophische Betrachtung der Ontologie von Medien. Dabei entwirft sie unter Bezugnahme auf Gilbert Simondons Technikphilosophie ein Gegenprogramm zu der von Bernhard Siegert vertretenen kulturtechnischen Analyse, und tritt mit seinem Artikel *Öffnen, Schließen, Zerstreuen, Verdichten. ›Operative Ontologien‹ der Kulturtechnik*, der in derselben Ausgabe der *Zeitschrift für Medien und Kulturforschung* erschienen ist, in einen Dialog. Deuber-Mankowsky weist auf die Differenzen von Ontologie und Ontologien hin: Verhandelt das philosophische Konzept der *Ontologie* die Frage nach dem Sein, so ist das informatische Konzept der *Ontologien* an der Operationalisierbarkeit von Wissen interessiert. Eine unscharfe Vermengung beider Begrifflichkeiten miteinander führe zu einer Übertragung der Bedeutungszusammenhänge aus einer informatischen Ordnung in eine medienwissenschaftliche, und damit, wie Deuber-Mankowsky (ebd., 160) mit Williard Quine deutlich macht, zu einem *ontologischen Debakel*, also einer »Operationalisierung [der analytischen Begrifflichkeiten, MS]: die Präzisierung und Standardisierung der Prozesse mit dem Ziel, sie verwendbar zu machen, und das heißt, als Algorithmen zu reformulieren und zu automatisieren.« Dies sorge in letzter Konsequenz dafür, über eine Unschärfe in der Theoriebildung eine Re-Ontologisierung

---

5 Ein zögerlicher erster Versuch lässt sich in der Abschaffung der »master/slave«-Terminologie in verschiedenen Programmiersprachen erkennen. In der Programmiersprache *Python* wurden diese Begriffe durch »parent/helper« ersetzt (vgl. Oberhaus 2018), bei dem Dateisystem *OpenZFS* durch »master/dependents« (vgl. Salter 2020). Da an den jeweiligen Funktionsweisen nichts verändert wurde, lässt sich diese Unternehmung mit McPherson jedoch eher als Kosmetik einstufen, und etwas optimistischer als den Beginn einer wünschenswerten Veränderung.

von Medien, sowie ein instrumentelles Technikverständnis einzuziehen, in dem Technik als scheinbar restlos Beherrschbares erscheint, als bloßes Werkzeug, das wiederum zur Beherrschung einer als passiv konzipierten Natur verwendet werden könne (vgl. ebd., 163–164, 167). Der Kern dieser Argumentation findet sich ebenfalls in dem rezent erschienenen Artikel *»Für eine Maschine gibt es kein echtes Virtuelles«. Zur Kritik des Smartness Mandate mit Felwine Sarrs Afrotopia und Gilbert Simondons Philosophie der Technik*. Dort weist Deuber-Mankowsky (2020) anhand einer Diskussion von Orit Halperns, Robert Mitchells und Bernard Dionysos Geoghegans These, dass das Konzept der Smartness das Konzept der Rationalität beerbe, darauf hin, dass daraus nicht folge, dass Rationalität ausschließlich als algorithmische Rationalität gedacht werden müsse oder könne, denn dies würde bedeuten, von einer immer schon algorithmisch bestimmten Zukunft auszugehen. Diese Geste lässt sich im Sinne der Queertheoretikerin Eve Kosofsky Sedgwick (2003, 124) als *reparativ* verstehen: Ein Verständnis für einen Sachverhalt »does not intrinsically or necessarily enjoin that person to any specific train of epistemological or narrative consequences.« Der Einsatz von Sedgwicks Aufsatz *Paranoid Reading and Reparative Reading, or, You're So Paranoid, You Probably Think This Essay Is About You* besteht darin, eine Art des Denkens und der Perspektivierung zu kultivieren, die sie als reparativ bezeichnet. Eine reparative im Gegensatz zu einer paranoiden Perspektive ermögliche es marginalisierten Personen innerhalb einer Gesellschaft, die ihnen kein Platz zugesteht, nicht nur zu überleben, sondern auch ein *gutes* Leben[6] führen zu können. Auf eine ähnliche Weise macht Deuber-Mankowsky (2020, 132) deutlich, dass es bei der Frage nach der Geschichtlichkeit des Rationalitätsbegriffs in letzter Konsequenz um »Fragen der Verteilung, der Solidarität, der Ungerechtigkeit und Ungleichheit« geht, sowie um die »Glücks- und Überlebensansprüche von einzelnen Individuen«. Im Verlauf ihres Aufsatzes legt sie dar, dass technische Funktionsweisen und medienphilosophische Betrachtungen derselben unterschiedlichen Rationalitäten, das heißt, unterschiedlichen »Regeln und Prozessen« (ebd., 135) folgen, und die jeweiligen Wissensbestände damit unterschiedlichen Ordnungen angehören. Eine Vermischung derselben, indem ehemals philosophische Konzepte in die Informatik überführt und von dort erneut in die Medienwissenschaft übertragen werden, hat eine Bedeutungsverschiebung zufolge.

---

6 Die gewählte Formulierung des *guten* Lebens bezieht sich an dieser Stelle explizit nicht auf die Fantasie des *guten Lebens*, die Lauren Berlant (2011) in *Cruel Optimism* bespricht.

Dieses »ontologische Debakel«, bei dem philosophische Konzepte operationalisierbar gemacht werden, führe einerseits zu einem instrumentellen Technikbegriff, und andererseits zu einer deterministischen Weltsicht, in der die Zukunft als geschlossen und schicksalhaft erscheint. Um stattdessen mögliche Zukünfte offen zu halten, gilt es also, eine ungenaue Übertragung von Konzepten zwischen diesen Bereichen, die Deuber-Mankowsky (ebd., 136) mit Walter Benjamin als in einer »diskontinuierliche[n] Struktur« verbunden beschreibt, zu vermeiden.

1.4 *Mit* der Technik schreiben

Was bedeuten diese Überlegungen für die vorliegende Arbeit? Sowohl McPherson als auch Deuber-Mankowsky thematisieren Übertragungen zwischen unterschiedlichen Rationalitäten, wobei jeweils mögliche Zukünfte auf dem Spiel stehen. Um diese im Plural und offen zu halten, muss große Sorgfalt in der Begriffsarbeit erfolgen, und müssen die jeweiligen Verschiebungen nachgezeichnet werden, die Konzepte wie Sicherheit oder Körperlichkeit erfahren, wenn sie von einer Rationalität in eine andere übertragen werden. Als das Offenhalten von Zukünften lässt sich auch der Einsatz der Queer Theory beschreiben, die in der vorliegenden Untersuchung vor allem mit Eve Sedgwicks (2003) Überlegungen zu paranoiden und reparativen Formen der Wissensproduktion im Hinblick auf die Diskussion der Herstellungspraktiken von Sicherheit in digitalen Kulturen zur Anwendung kommt. Während paranoide Praktiken der Wissensproduktion auf die Vermeidung von (negativen) Überraschungen hin ausgerichtet seien, komme den reparativen Praktiken die Offenhaltung von Zukünften zu. Diese beiden Formen der Wissensproduktion, sowie Sedgwicks bereits zitierte Bemerkung, dass eine bestimmte Art, Wissen über die Welt zu generieren, eine Person nicht deterministisch an die epistemologischen Konsequenzen dieser Form binde, werden im Verlauf dieses Buchs vor allem im Hinblick auf die Frage danach relevant, ob sich ein alternativer Sicherheitsbegriff für die Herstellung von Sicherheit in und mit digitalen Kulturen finden lässt. So versucht auch die vorliegende Untersuchung, in Sedgwicks Sinne reparativ zu agieren.

Weiterhin kann die von McPherson beobachtete Kompliz_innenschaft mit Technik aufzubrechen, aber dabei nicht in eine technikfeindliche Position zu verfallen, bedeuten, nicht nur *an* und *über* ›sichere‹ Computer zu schreiben, sondern *mit* ihnen – und konsequenter Weise nicht nur *über* Technik

zu schreiben, sondern *mit* ihr. *Mit* der Technik zu schreiben, bedeutet, die eigene Situierung in einer von Technik durchdrungenen Welt ernst zu nehmen, und nicht zu versuchen, die eigene Perspektive davon zu bereinigen. Vielmehr ermöglich ein solches, nicht instrumentelles Denken von Technik, die Verflechtung von (Medien-)Technik, Geschlecht und *race* scharf zu stellen. Die wechselseitige Konstitution dieser Felder falsifiziert schließlich die behauptete Trennung von techniknaher Medienwissenschaft und Geschlechterforschung, und öffnet den Blick für Medien als produktive Bestandteile diskursiver Formationen jenseits der ihnen zugeschriebenen deterministischen Programmierungen. In diesem Sinne möchte dieses Buch seine Leser_innen an den unterschiedlichen Prozessen und Regeln naturwissenschaftlich-technischer und geisteswissenschaftlicher Fachkulturen teilhaben lassen, aber auch aufzeigen, dass diese beiden Rationalitäten, ihren Unterschiedlichkeiten zum Trotz, in wechselseitig konstitutive Verhältnisse eintreten können und sich daher analytisch miteinander produktiv machen lassen. Ein Schauplatz, an dem dies in der vorliegenden Untersuchung geschieht, ist damit notwendiger Weise Sprache, sind Metaphern, sind Worte selbst. Auch Haraway (1997, 125) betont die Rolle von Sprache in ihren Überlegungen zu den *Science Wars*: »Words are weeds – pioneers, opportunists, and survivors. Words are irreducibly ›tropes‹ or figures. For many commonly used words, we forget the figural qualities; these words are silent or dead, metaphorically speaking.« Damit kommt Wörtern, und auch wissenschaftlichem Jargon, in Haraways Herangehensweise eine besondere Bedeutung zu: Wörter sind »thick, living, physical objects that do unexpected things« (ebd.) – und dies gilt nicht nur für Wörter, die auffallend metaphorisch oder bereits blumig klingen; auch »[m]athematical symbolisms and finely honed experimental protocols do not escape from the troping quality of any communicative medium […].« (Ebd.) Sie bemerkt weiter: »And, facts are tropic; otherwise they would not matter.« (Ebd.) *Matter* gilt hier im mehrfachen Wortsinn: In seiner Entsprechung als *bedeuten*, als *wichtig sein*, aber auch als *physische Substanz*. Um diese Amalgamierung pointiert zum Ausdruck bringen zu können, taucht schließlich der von Haraway oft gebrauchte Ausdruck »[m]aterial-semiotic« (ebd.) auf, oder im Deutschen: *materiell-semiotisch*. Auch die vorliegende Untersuchung ist reich an solchen materiell-semiotischen Figuren, die ins Denken bringen, und im Verlauf der Argumentation entfaltet werden.

In Kapitel 2 wird zunächst ein Überblick über die Geschichte der Kryptologie geschaffen. Nach einem kurzen Abriss der ersten 3000 Jahre der Kryptologie wird anhand von zwei *Schlüsselproblemen* in die mathematischen

Grundlagen sowie die innerfachliche Logik der Kryptographie eingeführt, sowie mit Sybille Krämer (2008; 2003) die Medialität von Kryptographie beleuchtet. Anschließend an die Diskussion *Moderner Kryptographie* (Katz/Lindell 2008) wird außerdem auf den der Kryptologie zugrunde liegenden Sicherheitsbegriff eingegangen, der mit Daniel Loick (2021) als negativer Sicherheitsbegriff bestimmt wird.

Kapitel 3 widmet sich anhand von Ransomware, Computerviren und -würmern der Herausbildung zeitgenössischer IT-Sicherheit in den 1980er Jahren, und zeichnet die Intersektionen des IT-Sicherheitsdiskurses mit dem HIV/AIDS-Diskurs nach. Eingeflochten in die Geschichte der Ransomware *WannaCry*, des *AIDS Information Trojaners* und der *Kryptovirologie* werden die titelgebenden unsicheren Kanäle besprochen, der Status der Übertragungen von HIV/AIDS-Metaphorik in den IT-Sicherheitsdiskurs untersucht, sowie letzterer als immunologisch strukturiert beschrieben. Anhand einer Gegenüberstellung der Praktiken zur Herstellung von Sicherheit in vernetzten Systemen mit Theoriebildung zu HIV/AIDS aus akademisch-aktivistischen Zusammenhängen der ACT UP-Bewegung wird auch der IT-Sicherheitsbegriff entgegen seiner zunächst an einem queeren Sicherheitsbegriff orientiert erscheinenden Praktiken *Safe Hex* und *Personal Systems Hygiene* als negativer Sicherheitsbegriff bestimmt.

Kapitel 4 befasst sich mit Backdoors als Figurationen digitaler Kulturen, die an der Intersektion von IT-Sicherheit und Kryptologie liegen, wodurch auch die Erkenntnisse aus den beiden vorangegangenen Kapiteln zusammengezogen werden. Im Anschluss an die Erläuterung der kleptographischen Backdoor in *DUAL_EC_DRBG*, die der Situierung von Backdoors innerhalb der Informatik dient, wird mit der Backdoor-Schadsoftware *Back Orifice* auf den homophoben Subtext von Backdoors eingegangen, und werden weiterführend mit Leo Bersani (1987) und Paul B. Preciado[7] (2015; 2003) zwei mögliche Umdeutungen desselben vorgeschlagen.

Kapitel 5 ordnet mit Eve Sedgwick die Praktiken der Wissensproduktion von Kryptologie und IT-Sicherheit, sowie den beiden Bereichen zugrunde lie-

---

7 Die Texte wurden noch nicht unter dem Namen Paul B. Preciado veröffentlicht. Da eine gewisse Nachvollziehbarkeit für Literaturnachweise gegeben sein muss, werde ich sie mit einem entsprechenden Hinweis gemäß den Angaben der jeweiligen Publikationen aufführen, im Text jedoch ausschließlich Paul B. Preciado nennen. Für weiterführende Überlegungen zu Zitation als scheinbar wertneutraler Praxis sowie akademischen Formen von *Care* siehe Thieme und Saunders (2018).

genden negativen Sicherheitsbegriff als paranoid strukturiert ein. Anschließend an die im vorangegangenen Kapitel vorgenommenen Umdeutungen von *Back Orifice* und der sich daraus ergebenden Frage, ob Sicherheit in digitalen Kulturen auch nicht negativ bestimmt werden könnte, schlägt das Kapitel mit Loick (2021) einen queeren Sicherheitsbegriff vor. Inwiefern dieser sich für Sicherheit in digitalen Kulturen produktiv machen lässt, wird anhand einer Diskussion von *QueerOS* und *Queer Computation* (vgl. Barnett et al. 2016; Gaboury 2018; Keeling 2014) im Hinblick auf reparative Praktiken und der Offenhaltung von Zukünften herausgearbeitet.

Abschließend bleibt an dieser Stelle mit Haraway (1997, 125) noch zu bemerken, dass, wenn Geschichtenerzählen einen elementaren Teil der Lebenswissenschaften darstellt, was »no insult, and certainly no dismissal« sei, dies auch auf dieses Buch zutrifft: »Stories are not ›merely‹ anything. Rather, narrative practice is one of the very odd and compelling parts of the semiosis of making […] knowledge.« (Ebd.) Es folgen also Geschichten über Sicherheit, Zahlenspiele, Viren, Würmer, über HIV/AIDS, Erpressung, das Eintreten durch Hintertüren und unsichere Kanäle.

2. Kryptographische Sicherheitsbestimmungen

»Ist das sicher?« Diese Frage ist früher oder später Teil von Unterhaltungen über (neue) Apps, Programme, Funktionen oder technische Endgeräte, und wurde mir, je länger ich mich mit IT-Sicherheit befasst habe, umso häufiger von Kolleg_innen, Freund_innen und Familienmitgliedern gestellt. Es gibt viele Möglichkeiten, diese Frage zu beantworten: Man könnte sich die AGB und Angaben zum Datenschutz eines jeweiligen Herstellers durchlesen und versuchen, nachzuvollziehen, was mit den Daten passiert, die bei der Benutzung einer App entstehen. Man könnte sich – sofern es sich um eine Open Source-Anwendung handelt – um einen Blick in den Quelltext bemühen, und versuchen zu überprüfen, ob die Anwendung bisher unbemerkte Sicherheitslücken enthält. Man könnte sich darüber informieren, ob eine App, beispielsweise ein Messenger, die bei der Benutzung entstehenden Daten verschlüsselt, und wenn ja, welche Verschlüsselungsmechanismen es gibt, und wie die verwendete Art der Verschlüsselung im Vergleich zu anderen abschneidet. Man könnte ein Gerät auseinander bauen, um sich zu vergewissern, dass die Hardware nicht manipuliert wurde. Man könnte… Diese Liste ist viel zu kurz, um alle Antwortmöglichkeiten zu beinhalten. Darüber hinaus setzen alle bisher angeführten Möglichkeiten auf verschiedenen Ebenen an, und unterschiedliche Kompetenzen voraus, die von dem Verständnis juristischer Texte wie AGBs bis hin zu den technischen Eigenschaften von Soft- und/oder Hardware reichen. Was in diesen Antwortmöglichkeiten nicht explizit angesprochen, aber durch die Auflistung sichtbar wird, ist die implizite Frage nach der Bedeutung des Wortes *sicher.* Denn nicht nur werden in dieser Aufzählung unterschiedliche Kompetenzen vorausgesetzt, sondern mit ihnen wird Sicherheit auch auf unterschiedlichen Ebenen verhandelt: auf rechtlicher Ebene (AGB), auf technischer Ebene (Vergleich von Verschlüsselungsmethoden, Untersuchen der Hardware) und auf der Ebene von Herstellungspraktiken (Open Source). Diese Ebenen sind bei der Herstellung von IT-Sicherheit, um die es im weitesten

Sinne bei der Frage nach Sicherheit in digitalen Medien geht, miteinander verknüpft. Die Annäherung an die Frage, was (IT-)Sicherheit bedeutet, wird im Folgenden zunächst über die Geschichte der Kryptographie vollzogen, da diese in bisherigen medienkulturwissenschaftlichen Betrachtungen von digitalen Phänomenen mit Bezug zu IT-Sicherheit, wie beispielsweise Computerviren, kaum bis gar nicht beachtet wurde,[1] aber grundlegend für das Verständnis von IT-Sicherheit ist. Von besonderem Interesse für die weiteren Ausführungen ist daher auch eine genauere Betrachtung der Intersektion von Kryptographie und Informatik, und der daraus folgenden Übertragung kryptographischer Sicherheitskonzepte in die Informatik, die den Bereich der IT-Sicherheit sowohl in der Industrie als auch als wissenschaftliche Disziplin kennzeichnet.

In diesem Kapitel soll daher zunächst ein wissensgeschichtlicher Überblick über zentrale Konzepte in der Geschichte der Kryptographie gegeben werden, die jeweils im Hinblick auf ihre Medialität sowie das zugrunde liegende Konzept von Sicherheit diskutiert werden. Anschließend wird im folgenden Kapitel eine wissensgeschichtliche Betrachtung dessen, was heute in der IT-Sicherheit unter Sicherheit verstanden werden kann, entfaltet werden. Für diesen Zweischritt ist eine artifizielle Aufteilung der Anwendungsbereiche von Kryptographie in zwei Bereiche notwendig: Erstens die Sicherheit von Kommunikationsinhalten während des Kommunikationsvorgangs und zweitens die Sicherheit von (vernetzten) IT-Systemen abseits von Kommunikationsprozessen menschlicher Akteur_innen.[2] Diese Trennung

---

1 So findet Kryptographie beispielsweise in Jussi Parikkas (2016) *Digital Contagions. A Media Archaeology of Computer Viruses* keine Erwähnung. Alexander Galloway und Eugene Thacker (2007, 86–87) streifen in *The Exploit. A Theory of Networks* Kryptographie als Eigenschaft sowohl von biologischen Viren als auch von Computerviren, allerdings eher in einem (schiefen) metaphorischen Sinne, da sie das kryptographische Element von Viren daran festmachen, dass diese sich stets veränderten. Während Galloway und Thacker zwar die prozessuale Eigenschaft von Kryptographie erkennen, ist das Ziel von Kryptographie jedoch, wie sich im Folgenden herausstellen wird, eine Remediatisierung mit möglichst geringer Veränderung des Inhaltes. Der Gebrauch des Worts Kryptographie bei Galloway und Thacker folgt also eher einer »occult cryptography« (ebd., 129), die in die Richtung einer Numerologie zeigt.

2 Letzteres betrifft einerseits bereits gespeicherte Daten, sowie andererseits das ungestörte Funktionieren vernetzter Computer. Der Aspekt der Stabilität und Verfügbarkeit durch die regelmäßige Wartung von Systemen wird in diesem Buch nicht thematisiert, da er, mehr als die anderen beiden Aspekte, an konkreten Praktiken im Sinne von Heuristiken und *best practices* orientiert ist, und daher einerseits über eine schlechte wis-

dient ausschließlich der Vermittelbarkeit dieser komplexen Geschichte in zwei Erzählsträngen: Erstens der Geschichte der Kryptographie, die in diesem Kapitel besprochen wird, und der darin liegenden Abgrenzung *moderner* von *klassischer* Kryptographie, sowie zweitens deren Anwendungsfelder in der IT-Sicherheit, die im nachfolgenden Kapitel diskutiert werden. Diese Einteilung wird sich bereits im Verlauf des vorliegenden Kapitels an manchen Stellen als brüchig erweisen, was gleichsam als Nachweis der Künstlichkeit der von mir eingezogenen Trennung verstanden werden kann. Da dies jedoch immer noch eine nur unzureichende Beantwortung der Frage danach ist, was *sicher* in den jeweiligen Fällen und Diskursen bezeichnet, wird außerdem darauf eingegangen, welche Aussagen darüber, wie Sicherheit funktioniert, was sie leisten kann und soll, vom mathematisch-technischen Diskurs unausgesprochen bleiben.

2.1 Zum Status des Wissens über Kryptographie

Die Geschichte der Kryptographie ist, gemessen an ihrer langen Existenz, erst vor kurzem geschrieben worden. David Kahn, der Autor des kanonischen Buchs *The Codebreakers. The Story of Secret Writing*, bemerkt dazu im Vorwort desselben:

> »CODEBREAKING is the most important form of secret intelligence in the world today. It produces much more and much more trustworthy information than spies, and this intelligence exerts great influence upon the policies of governments. Yet it has never had a chronicler. It badly needs one.« (Kahn 1967, ix)

Kahns Buch wurde 1967 veröffentlicht, inmitten des Kalten Krieges, und nur wenige Jahre vor Ende des Vietnamkrieges. Wie bereits aus dem kurzen Zitat aus dem Vorwort zu erkennen ist, erzählt Kahn die Geschichte der Kryptographie als Militärgeschichte. Die zahlreichen Beispiele – Kahn (ebd.) legt mit *The Codebreakers* die, in seinen Worten, »entire history of cryptology« vor – befassen sich also mit der Rolle von Kryptographie in Kriegshandlungen, in Konflikten zwischen Staaten, als Werkzeug von Botschaftern und Spionen.

senschaftliche Quellenlage verfügt, und andererseits außerhalb dessen liegt, was eine qualitative medienwissenschaftliche Arbeit leisten kann.

Entsprechend beginnt das erste Kapitel in medias res: Mit einer Nachricht zunächst unbekannten Ursprungs an den japanischen Botschafter in den USA, die in den frühen Morgenstunden des 7. Dezember 1941 von der US-amerikanischen Navy abgefangen und entschlüsselt wurde. Die Nachricht wies den japanischen Botschafter an, der US-amerikanischen Regierung einen einige Stunden zuvor in 14 Teilen gesendeten Beschluss der japanischen Regierung mitzuteilen: Dass diese sich außerstande sehe, durch weitere Verhandlungen mit den USA zu einer diplomatischen Lösung des Konflikts der beiden Staaten zu kommen (vgl. ebd., 2). Die Beziehungen von Japan und den USA waren bereits seit längerem konfliktbehaftet, und sollten an diesem Tag in dem Angriff japanischer Soldaten auf Pearl Harbor kulminieren, und das, wie Kahn (ebd., 4) herausstellt, *obwohl* es den USA gelang, die abgefangenen Nachrichten zu dekodieren, was er schließlich darauf zurückführt, dass in der dekodierten Nachricht keine Pläne für einen Angriff enthalten waren. Kahns Erzählungen der Ereignisse lesen sich für einen wissenschaftlichen Text nahezu übermäßig szenisch, fast wie ein Spionage-Thriller, was zweifelsohne dazu dienen soll, jeden Verdacht darauf zu zerstreuen, dass mathematische Entwicklungen eine trockene Materie seien.

In Kahns Tradition steht, sowohl was den Schreibstil als auch die Rahmung von Kryptographiegeschichte als Militärgeschichte angeht, auch Simon Singhs *The Code Book. Science of Secrecy from Ancient Egypt to Quantum Cryptography*, das ungefähr 30 Jahre später, kurz vor der Jahrtausendwende erstmals veröffentlich wurde. »For thousands of years«, so beginnt Singhs (2000, xiii) Einleitung,

> »kings, queens and generals have relied on efficient communication in order to govern their countries and command their armies. At the same time, they have all been aware of the consequences of their messages falling into the wrong hands, revealing precious secrets to rival nations and betraying vital information to opposing forces. It was the threat of enemy interception that motivated the development of codes and ciphers: techniques for disguising a message so that only the intended recipient can read it.«

Die historisch gewachsene, enge Verknüpfung von Kryptographie und Kriegsführung sowie Spionage soll an dieser Stelle nicht nur als eine mögliche Art der Diskursivierung durch die Autor_innen dieser Geschichte abgetan werden, sondern hat Auswirkungen auf das Wissen, das über Kryptographie gewusst und hergestellt werden kann. Auf diesen Umstand nimmt ein – verglichen mit Kahn und Singh – eher unbekanntes, aber dennoch sehr genaues und

hilfreiches Buch Bezug, das an dieser Stelle ebenfalls erwähnt sein soll: Friedrich Bauers *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Bauers Buch ist vor allem aufgrund seiner Situierung im deutschen akademischen Kontext spannend, innerhalb dessen er zu Beginn der 1980er Jahre die erste öffentliche Vorlesung an einer westdeutschen Hochschule mit dem Titel »Kryptologie« hielt (vgl. Bauer 1997, V). Nach einer scherzhaft erzählten Anekdote darüber, dass Bauer eine Einmischung seitens deutscher Behörden in seinen Unterricht befürchtete, und er eines Tages tatsächlich die »unbekannten Gesichter zweier mittelalterlicher Herren mit Anzügen« (ebd., VI) in seiner Vorlesung erblickte – ein Vorkommnis, das ungeklärt blieb – schreibt Bauer (ebd., VI–VII) in der Einleitung seines Buchs weiter:

> »Ich bin es dem Leser nun doch schuldig, zu erklären, woher mein Interesse an der Kryptologie und meine Vertrautheit mit ihr herrührt. Vorab, mein größter Vorteil ist, daß ich nie Angehöriger eines Dienstes war. Ich stehe also unter keiner irgendwie gearteten Schweigepflicht. [...] Trotzdem weiß ich nie, ob ich das, was ich weiß, auch wissen darf.«

Die Verstrickung von Geheimdiensten oder anderen staatlichen Akteur_innen in die Wissensproduktion in der und über die Kryptographie thematisiert auch David Kahn in seinem Vorwort mit einem kurzen Hinweis darauf, dass sein Buch vor Veröffentlichung dem *Department of Defense* zugegangen sei. Dies lässt darauf schließen, dass Kahn sicherstellen musste, keine *classified information* zu veröffentlichen – was allerdings an dieser Stelle eine Spekulation meinerseits (und vermutlich auch anderer Leser_innen) ist, da Kahn sich nicht zum Zweck dieser Vorlage äußert. Auch Singh (2000, xvi) weist auf die Prekarität des Wissens über Kryptographie hin, wenn er schreibt, »I must mention a problem that faces any author who tackles the subject of cryptography: the science of secrecy is largely a secret science.« Im Gegensatz zu Kahn findet bei Singh keine Kontrolle durch staatliche Akteur_innen Erwähnung, allerdings verweist er darauf, für seine Forschung wichtige Daten direkt vom britischen Geheimdienst GCHQ bekommen zu haben, und dass diese erst kurz vorher freigegeben wurden. Doch diese Unterstützung deutet auch darauf hin, so schreibt er weiter, dass Geheimdienste »such as GCHQ and America's National Security Agency continue to conduct classified research into cryptography, which means that their breakthroughs remain secret and the individuals who make them remain anonymous« (ebd., xvii). Eine Geschichte der Kryptographie steht aufgrund ebendieser Geheimhaltungspraktiken notwendigerweise stets unter Verdacht, nicht auf der Höhe

der Zeit zu sein, nicht alle Entwicklungen und Akteur_innen bedacht haben zu können – dies gilt damit ebenso für die vorliegende Publikation. Doch Singh weicht auch in einigen Punkten von dem militärischen Narrativ ab, vor allem in der Darstellung von kryptographischen Entwicklungen der späten 1970er Jahre wie der Public Key-Kryptographie. Weshalb diese Verschiebung in der Erzählweise möglich ist, wird unter anderem Gegenstand dieses Kapitels sein.

2.2 Zur Medialität von Kryptographie

Die bisherigen Überlegungen stützen sich maßgeblich auf Literatur aus dem Feld der Kryptographie selbst, sowie auf Quellen von Historikern. Dies ist zwar eine reichhaltige Materialgrundlage, aber dennoch auch keine zufällige Auswahl: Die Menge geisteswissenschaftlicher Forschung zu Kryptographie ist recht überschaubar, und oft wird Kryptographie nur im Zuge eines anderen Themas begleitend gestreift.[3] Eine nennenswerte Ausnahme ist Quinn DuPonts (2017) unter dem Namen *An Archeology of Cryptography: Rewriting Plaintext, Encryption, and Ciphertext* veröffentlichte Dissertation, die Kryptographie aus medienarchäologischer Perspektive betrachtet. Während sowohl DuPonts Arbeit als auch die vorliegende sich gegen ein instrumentelles Technikverständnis wenden und an diskursiven Möglichkeitsbedingungen von Kryptographie interessiert sind, schlagen sie doch differente Wege ein. DuPont situiert Kryptographie vorrangig in Hinblick auf Notation, d.h. Schrift, Schreiben und dessen Materialität, und fokussiert vor allem die Relation von Kryptographie und Sprache. An den technischen und mathematischen Details kryptographischer Systeme, ebenso wie an der jüngeren Geschichte der Kryptographie ist DuPont im Gegensatz zur vorliegenden Untersuchung jedoch

3 In *What is Media Archaeology?* diskutiert Jussi Parikka (2012, 90–112) kurz das Erstarken der Kryptographie im 19. Jahrhundert und ihren Zusammenfall mit der Telegraphie, wobei es ihm hauptsächlich um das Phänomen *Noise* geht. Friedrich Kittler (1986, 378–379) erwähnt Kryptographie in *Grammophon, Film, Typewriter*, allerdings im Zuge der kulturpessimistischen Diagnose, dass die Kryptographie eine automatisierte Diskursanalyse zur Folge habe. Alexander Galloway und Eugene Thacker (2007) streifen, wie bereits erwähnt, in *The Exploit* Kryptographie als Konzept, um auf Viren einzugehen. Die Performerin und Philosophin Susan Kozel geht in zwei Artikeln, die ihre eigenen Performanceprojekte diskutieren, auf die für die Performances zentrale prozessuale Dimension asymmetrischer Verschlüsselung ein (vgl. Kozel 2017; 2016).

nicht interessiert, weswegen sich die Pfade unserer Betrachtungen im Weiteren kaum kreuzen werden. Den überschaubaren geisteswissenschaftlichen Forschungsstand zu Kryptographie bespricht allerdings auch DuPont (2020) in seinem Aufsatz *Cryptographic Media*: »Despite the phenomenal rise in the use of cryptography, the emergence of a trillion-dollar computer security industry, unprecedented government interest and investment, and daily news stories describing the horrors of an insecure or overly secure Internet«, führt DuPont (ebd., 692) aus, »academic work on cryptographic media has tended to focus on a few important but limited areas of investigation.« Diese Felder seien zumeist, und diese Aussage bestätigte sich in meiner Recherche, Informatik, Ingenieurswissenschaften, und die Kryptographie als Disziplin selbst. Die Forschung in diesen Bereichen bezeichnet DuPont (ebd.) als »massive and well-funded«, sowie in vielen Fällen »cozy with corporate and government sponsors« – dies ist zweifelsohne ein Umstand, der sich darauf auswirkt, welches Wissen gewusst, produziert wird und werden kann.[4] Angesichts dieser Förderungssituation, schreibt DuPont (ebd.) weiter, könne man fälschlicherweise glauben, »cryptographic media« seien ausreichend beforscht und verstanden, doch das Gegenteil sei der Fall. DuPont (ebd., 692–693) macht große Wissenslücken in der Forschung, vor allem auf Seite der Geisteswissenschaften aus:

> »We might wonder, then, why have important questions not yet been *asked*? For instance, what *is* cryptography? Technologists, mathematicians, and engineers have answers, but they are not very satisfying – either doing too little or too much (the common plea that cryptography is just math is so broad that it risks explaining everything and nothing). Either way, these answers lack social and human richness. […] why, given its ubiquity, is encryption not considered one of the fundamental media technologies of the twentieth cen-

4 DuPont geht bis auf diese spitze Bemerkung nicht weiter auf die Förderungssituation mathematisch-naturwissenschaftlicher Fächer ein. Eine der wenigen Stimmen innerhalb der Kryptographie, die diesen Umstand kritisch diskutiert, ist Phillip Rogaway. In seinem Vortrag *The Moral Character of Cryptographic Work* greift Rogaway (2015, 37) die scheinbare Neutralität kryptographischer Forschung, die sich vornehmlich mit Zahlen und Rätseln befasse, angesichts ebendieser Nähe kryptographischer Forschung zu Geheimdiensten, Militär und Industrie an: »The military funding of science invariably redirects it and creates moral hazards. […] No matter what people say, our scientific work does change in response to sponsor's institutional aims.«

tury (alongside radio, telephone, and television), and how do we explain its emergence and its future?«

DuPonts Artikel liefert einen Überblick über die Auseinandersetzung mit Kryptographie in den Bereichen Medienwissenschaft, Science and Technology Studies und Software Studies, und konstatiert, dass alle bisherigen Auseinandersetzungen unzureichend seien: Es fehle ein »sufficient theoretical framework for cryptography« (ebd., 693). Während DuPont (ebd.) zuzustimmen ist, was die überschaubare Quellenlage angeht, so kann es nur als Polemik aufgefasst werden, wenn er gleich drei Forschungsfeldern die naive Haltung unterstellt, sich bisher nicht mit Kryptographie auseinandergesetzt zu haben, da diese vermutlich glaubten, »that encrypted communication changes nothing, since, after all, encrypted communication is usually decrypted at its terminal location, seemingly returned to its original.« Der von ihm eigeforderten »cryptographic media theory« (ebd.) möchte dieses Buch dennoch nicht entsprechen, da die ersten richtungsweisenden Vorschläge, die DuPont im diskutierten Artikel für eine solche *cryptographic media theory* macht, in die Richtung einer weiteren Spielart kulturtechnischer Betrachtungen zeigen. Das vorliegende Buch wird daher den Blick nicht auf Kryptographie, also Verschlüsselung, *als Medium* (als »one of the fundamental media technologies of the twentieth century (alongside radio, telephone, and television)«) richten, da eine solche Betrachtungsweise Gefahr läuft, die Leistung von Verschlüsselung stillzustellen und damit zu verkennen, sondern fokussiert die prozessuale Dimension, *die Medialität*, von Ver- und Entschlüsselung, von Kryptographie. Was ist damit gewonnen?

Zunächst lässt sich festhalten, dass die »Annahme, es gebe Einzelmedien«, sich mit Sybille Krämer (2003, 85) als »Resultat einer Abstraktion« begreifen lässt, die zu der für die Medientheorie zentralen Frage führt, ob Medien Sinn erzeugen oder vermitteln. Krämer nähert sich dieser Frage in ihrem Aufsatz *Erfüllen Medien eine Konstitutionsleistung? Thesen über die Rolle medientheoretischer Erwägungen beim Philosophieren* davon ausgehend, dass die Bestimmung dessen, was Medien sind, sich weder in den Zeichen, die sie übertragen, noch in den Gegenständen und technischen Apparaten, die ihre Materialität ausmachen, erschöpft (vgl. ebd., 79). Im Verlauf ihres Aufsatzes legt Krämer eine philosophische Reflexion von Medien und Medialität vor, die Medien als konstitutive Elemente für das, was sie vermitteln, und damit auch des Denkens und des Philosophierens wahrnimmt, ohne dabei ein mediales Apriori anzu-

nehmen. Wie eine solche Denkweise von Medien aussehen kann, etabliert sich, wie Krämer (ebd., 80) formuliert,

> »zwischen zwei Polen: Der eine Pol ist die (traditionell geisteswissenschaftliche) Auffassung von der ›Sekundarität des Medialen‹: Ausgehend von der Vehikelfunktion, vom transitorischen, vermittelnden Charakter des Mediums werden Medien mit den materiellen Realisierungsbedingungen symbolischer Formen/Gehalte identifiziert. Medien übertragen etwas, das selbst nicht ›von der Natur eines Mediums‹ ist, sei das nun der Gehalt, die Botschaft, der Sinn oder die Form. Es gibt also ein Außerhalb von Medien. Der andere Pol ist die (eher kulturalistisch inspirierte) Auffassung vom ›Primat des Medialen‹: Medien gelten dann […] als zeitgenössische Fortbildung eines Sprach-, Zeichen- oder Technikapriori. […] Es gibt kein Außerhalb von Medien.«

An diesem Punkt stellt sich die »Gretchenfrage« (ebd.) der Medientheorie: Übermitteln oder erzeugen Medien etwas? Die beiden von Krämer beschriebenen Pole entstehen durch die für Medien charakteristische Eigenschaft, einen Unmittelbarkeitseindruck durch ihren Entzug herzustellen: Gelingt die Vermittlungsleistung, so werden Medien unsichtbar. Nur in ihrer Störung treten Medien an Stelle ihres Inhaltes wieder in Erscheinung (vgl. ebd., 81). Weiterhin unterscheidet Krämer (ebd.) zwischen Medium und Medialität, und setzt dazu im Anschluss an Niklas Luhmann Medien als »Unterscheidungs-Potenziale« ein: »Sie stellen ein Strukturierungsrepertoire bereit, das zur Formbildung dient.« In Absetzung von Luhmanns systemtheoretischer Perspektive sind die medialen Akte der Formgebung für Krämer (ebd.) allerdings keine »Operationen eines Systems«, sondern vielmehr »kulturelle Praktiken« – was sich als Medien beschreiben lässt, ist folglich eine Art geronnener Kultur. Als bedeutsam für diese Sichtweise von Medien führt Krämer zwei Momente an: Erstens, dass die Unterscheidung von Medium und Form nicht statisch sei, sondern stets abhängig von dem Erkenntnisinteresse und der eingenommenen Perspektive auf den analysierten Gegenstand; und zweitens, dass Medien sich nicht nur durch eine Störung, sondern auch dort nicht mehr der Wahrnehmung entziehen, wo sie zur Form werden, die in einem anderen Medium erscheint (vgl. ebd., 82). Eine ähnliche Beobachtung machen auch Jay David Bolter und Richard Grusin (2000) mit dem von ihnen geprägten Begriff der *Remediation*, der im Folgenden verwendet wird, um die Aufnahme eines Mediums in ein anderes Medium zu beschreiben. Bolter und Grusin stellen ebenso wie Krämer fest, dass Medien sich einerseits der Wahrnehmung

entziehen und so eine durch den Eindruck von Unmittelbarkeit gekennzeichnete Erfahrung herstellen, was sie als *immediacy* bezeichnen (vgl. ebd., 70). Gleichzeitig gehe mit der Aufnahme eines Mediums in ein anderes Medium einher, dass man sich – vermittelt über die Differenz zum alten Medium – des Neuen gewahr werde, was sie als *hypermediacy* beschreiben (vgl. ebd., 34). In dieser »double logic of remediation« (ebd., 55) nehmen Medien darüber hinaus stets aufeinander Bezug, ohne dabei zwangsläufig eine zeitlich lineare Genealogie zu bilden: Nicht nur neue Medien können ältere remediatisieren, auch ältere Medien können neuere remediatisieren (vgl. ebd.). Bolters und Grusins Modell der Remediation eignet sich damit nicht für eine historisierende Betrachtung von Medien, stellt aber in der Logik, dass Remediation »*the mediation of mediation*« ist, eine analytische Herangehensweise zur Verfügung, die es erlaubt, Mediatisierungsprozesse in den Blick zu nehmen, und Medien als interdependent zu verstehen: »Each act of mediation depends on other acts of mediation. Media are continually commenting on, reproducing, and replacing each other, and this process is integral to media. Media need each other in order to function as media at all.« (Ebd.) Ein ähnlicher Einsatz findet sich bei Krämer (2003, 85), die konstatiert: »Immer geht dem Medium etwas voraus; doch das, was ihm vorausgeht, ist zwar in einem anderen Medium, nie aber ohne Medium gegeben.« An dieser Stelle benennt Krämer das von ihr vertretene Programm als *Metaphysik der Medialität*, die als Gegenprogramm zu einer von einem Medienapriori ausgehenden Medienontologie fungiere.[5] Die Metaphysik sei keine universale, wie Krämer (ebd., 82) schreibt, da über Medialität nachzudenken auch heiße, über Perspektivität nachzudenken. So lässt sich Krämers Medialitätsbegriff an Haraways Konzept des *Situierten Wissens* anschließen (vgl. Haraway 1991a). Die Fokussierung auf Medialität ermöglicht es Krämer darüber hinaus, über die Performativität von Medien nachzudenken. Diese liege darin begründet, dass Medien Dinge erscheinen lassen, und dabei das, was erscheint, »zugleich transformiert, manchmal

5 Krämer betont, dass eine nicht-essentialistische Sichtweise auf Medien eine Medienontologie ausschließe. Dies scheint auf den ersten Blick ein Widerspruch zu Deuber-Mankowskys Überlegungen zur Medienontologie zu sein. Bei näherer Betrachtung erweisen sich die beiden Ansätze jedoch als demselben Erkenntnisinteresse verschrieben, denn Deuber-Mankowsky (2017a, 166) zufolge zeige sich die Existenz von Medien jenseits eines medialen Apriori »in den Effekten, die sie durch ihre Teilnahme an Werdensprozessen zeitigen.« Medien sind demnach nicht apriorisch ontologisch gesetzt, sondern ihre Existenz lässt sich genau in den Effekten ihrer Medialität in den mediatisierten Dingen erkennen.

auch unterminiert« (Krämer 2003, 83) werde. Die Performativität des Medialen ziele auf eine Beschäftigung mit diesem »Überschuss« (ebd.) ab, der in der medialen Hervorbringung entstehe, und sich damit als Eigenleistung des Mediums konzeptualisieren lässt. Mit Anja Michaelsen (2018, 112) lässt sich an dieser Stelle noch hinzufügen, dass gerade dieser durch die »Betonung des Medienspezifischen und Materiellen« in den Blick rückende »ästhetische[…], sinnliche[…] Überschuss« ein zentrales Anliegen medienwissenschaftlicher Analyse ist, und sich für Fragestellungen aus der Geschlechterforschung produktiv machen lässt. In diesem Sinne soll DuPonts Frage, was Kryptographie eigentlich ist, durch eine Fokussierung der prozessualen Dimension, *der Medialität*, von Ver- und Entschlüsselung diskutiert werden, die sich auch, wie in dieser Untersuchung deutlich werden wird, ausgehend von mathematischen, technischen, und historischen Quellen bestreiten lässt.

2.3 *Klassische* und *moderne* Kryptographie

Es gibt verschiedene Definitionen dessen, was Kryptographie ist, die zwar nicht über denselben Wortlaut verfügen, aber grundsätzlich dasselbe Prinzip beschreiben: Singh (2000, xiv) definiert Kryptographie als »art of secret communication«, und Kahn (1967, xiii) gibt keine direkte Definition, verweist aber darauf, dass »methods of cryptography […] do not conceal the presence of a secret message but render it unintelligible to outsiders«. Aus dem Feld der Kryptographie selbst kommen folgende Definitionen: Neal Koblitz (2007, 979) definiert Kryptographie als »science of transmitting and managing information in the presence of an adversary«. Bauer (1997, 27) schreibt: »Die klassische Aufgabe der Kryptographie ist es, eine Nachricht oder Aufzeichnung für den Unbefugten unverständlich zu machen.« Oded Goldreich (2004, 2, Herv. i.O.) spezifiziert: »The problem of providing *secret communication over insecure media* is the most traditional and basic problem of cryptography.« Whitfield Diffie und Martin Hellman (1976, 645) setzen Kryptographie als »the study of ›mathematical‹ systems for solving two kinds of security problems: privacy and authentication.« Christof Paar und Jan Pelzl (2016, 2, Herv. i.O.) konstatieren in ihrem Lehrbuch *Kryptografie Verständlich*: »Die **Kryptografie** beschäftigt sich mit der *Absicherung* von Daten, z.B. der Verschlüsselung von Nachrichten.« Etymologisch setzt sich das Wort *Kryptographie* aus dem griechischen *κρυπτός* (»kryptós«) für verborgen, heimlich, geheim und *-γραφία* (»-graphia«, von γράφειν, »gráphein«: kerben, (ein)ritzen, schreiben, zeichnen) zusammen

(vgl. Dudenredaktion 2020, 423, 634), und könnte wörtlich etwa als *Geheimschrift* ins Deutsche übertragen werden. Das *Oxford English Dictionary* (2011) definiert *cryptography* als »1. The art or practice of writing in code or cipher; the science of encryption; the branch of cryptology concerned with this (cf. cryptanalysis n.). More generally: the study of codes and ciphers; cryptology«, und »2. Coded writing; a particular code or cipher. Also *figurative*.« Alle diese kurzen Definitionen nennen Teilaspekte dessen, was Kryptographie leistet, die für ein besseres Verständnis an dieser Stelle zusammengezogen werden sollen. Kryptographie ist, soviel geht aus den bereits genannten Definitionen hervor, mit dem Verschlüsseln von Inhalten befasst, die entweder als Nachrichten, Informationen, oder einfach als Kommunikation bezeichnet werden (dazu später mehr). Die Verschlüsselung macht besagte Inhalte für unbefugte Leser_innen unverständlich, verbirgt aber nicht ihre Existenz.

Sowohl Bauer als auch Paar/Pelzl ordnen Kryptographie, ausgehend von ihrem Oberbegriff Kryptologie, mittels eines Baumdiagramms ein. Bauer (1997, 26) unterschiedet an der ersten Verzweigung des Baumes zwischen offenen und gedeckten Geheimschriften: Offene Geheimschriften definiert er als »eigentliche Kryptologie«, verdeckte als »Steganographie«. Aus dieser Differenz erklärt sich Kahns Bemerkung, dass Kryptographie eine Nachricht unlesbar mache, aber ihre Existenz nicht verstecke – letzteres ist die Aufgabe der Steganographie (vgl. ebd., 9).[6] Während Bauer das Baumdiagramm lediglich auf der Seite der Steganographie weiter ausführt, lässt sich für den Bereich der »eigentlichen Kryptologie« mit Paars und Pelzls (2016, 3) Baumdiagramm anschließen, die Kryptographie und Kryptanalyse als erste Verzweigung unter dem Oberbegriff Kryptologie benennen. Mit Bauer (1997, 25) sei an dieser Stelle noch darauf verwiesen, dass der Begriff *Kryptologie*, trotz sporadischer früherer Verwendung, erst durch Kahns *The Codebreakers* als Oberbegriff für *Kryptographie* und *Kryptanalyse* fest etabliert wurde. Die Aufteilung von Kryptologie in zwei komplementäre Bereiche entspricht auch der genau gegensätzlichen Aufgabenverteilung der beiden: Ist Kryptographie mit dem Verschlüsseln von Nachrichten befasst, so geht es in der Kryptanalyse um das »*Brechen* von Kryptosystemen« (Paar/Pelzl 2016, 2, Herv. i.O.). Entgegen der Annahme, dass Kryptanalyse vornehmlich von Kriminellen oder Geheimdiensten praktiziert würde, weisen Paar und Pelzl (ebd., 2–3) darauf hin, dass es sich bei der Kryptanalyse durchaus um eine wissenschaftliche Disziplin

6 Auf Steganographie wird in diesem Buch nicht genauer eingegangen. Für einen ausführlichen Überblick über steganographische Methoden siehe Bauer (1997, 9–25).

handelt, deren Ergebnisse für die Kryptographie unabdingbar seien, und dass die meisten Kryptanalyst_innen Wissenschaftler_innen seien. Der Status von Wissenschaftlichkeit ist tatsächlich, und das mag aus heutiger Perspektive überraschen, auch für die Kryptographie nicht selbstverständlich. Die Kryptographen Jonathan Katz und Yehuda Lindell (2008, 3) gehen auf diesen zweifelhaften Status zu Beginn ihres Buchs *Introduction to Modern Cryptography* genauer ein, in dem sie eine *modern cryptography* von einer *classical cryptography* abgrenzen:

> »The Concise Oxford Dictionary (2006) defines cryptography *as the art of writing or solving codes*. This definition may be historically accurate, but it does not capture the essence of modern cryptography. First, it focuses solely on the problem of secret communication. This is evidenced by the fact that the definition specifies ›codes‹, elsewhere defined as ›a system of pre-arranged signals, especially used to ensure secrecy in transmitting messages‹. Second, the definition refers to cryptography as an art form. Indeed, until the 20th century (and arguably until late in that century), cryptography was an art.«

Obgleich die Definition des *Concise Oxford Dictionary*, gegen die sich Katz und Lindell wenden, im bereits zitierten *Oxford English Dictionary* um den Aspekt der Wissenschaftlichkeit erweitert ist, benennt auch dasselbe Kryptographie zuvorderst als »art or practice of writing in code or cipher«. Katz und Lindell konstatieren, dass das Verständnis von Kryptographie als Kunst bis ins späte 20. Jahrhundert gerechtfertigt sei, da es kaum wissenschaftliche Theoriebildung und damit kein Feld gegeben habe.[7] Dies habe sich jedoch mit dem Aufkommen *moderner Kryptographie*, das Katz und Lindell (ebd., Herv. i.O.) auf die 1980er Jahre datieren, verändert: »A rich theory emerged, enabling the rigorous study of cryptography as a *science*.« Anhand des Worts »rigorous«, das in Katz' und Lindells Buch noch sehr oft in beschreibender Funktion für die Genauigkeit von Methoden Verwendung findet, wird deutlich, dass die beiden Autoren die Wissenschaftlichkeit von Kryptographie nicht nur an

7 Ein ähnliches Argument macht auch Kahn (1967, 72), der darauf hinweist, dass die Entwicklung der Kryptologie in den ersten 3000 Jahren ihrer Geschichte schleppend und nicht linear verlaufen sei: »In its first 3,000 years, it did not grow steadily. Cryptology arose independently in many places, and in most of them it died the deaths of its civilizations. In other places, it survived, embedded in a literature, and from this the next generation could climb to higher levels. But progress was slow and jerky. More was lost than retained. Much of the history of cryptology of this time is a patchwork, a crazy quilt of unrelated items, sprouting, flourishing, withering.«

Theoriebildung, sondern vor allem an der Ausbildung von strengen Definitionen und Methoden festmachen. Kennzeichnend für die *moderne Kryptographie* ist Katz und Lindell folgend darüber hinaus ihr erweitertes Anwendungsgebiet: Moderne Kryptographie ist nun nicht mehr auf die Geheimhaltung von Nachrichten, und damit auf Kommunikationsakte beschränkt, sondern »deals with the problems of message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, digital cash and more« (ebd.). Diese Entgrenzung, die im Folgenden aus mediengeschichtlicher Sicht als maßgeblich mit der Entstehung des Internets zusammenhängend beschrieben werden kann, bringt auch eine erweiterte Nutzer_innenschaft mit sich und löst die Kryptographie aus ihrer vormals ausschließlich militärisch diskursivierten Geschichte. Gleichsam ist diese Entgrenzung an der Verschmelzung von Kryptographie und Informatik beteiligt, und damit an der Herausbildung von IT-Sicherheit als wissenschaftliche Disziplin. »Without attempting to provide a perfect definition of modern cryptography,« schreiben Katz und Lindell (ebd.), »we would say that it is *the scientific study of techniques for securing digital information, transactions, and distributed computations.*« Im Folgenden sollen die mediengeschichtlichen Entwicklungen betrachtet werden, die diese Verschiebung ermöglichten, sowie anhand konkreter Beispiele auf die Medialität kryptographischer Verfahren eingegangen werden.

2.4 Zwei Schlüsselprobleme der Kryptographie

1976 veröffentlichten Whitfield Diffie und Martin Hellman ein Paper mit dem Titel *New Directions in Cryptography*. Eines der Hauptprobleme, für das Diffie und Hellman (1976, 644) in ihrem Aufsatz eine Lösung anbieten, ist das Problem der Schlüsselverteilung, oder genauer: »the need for secure key distribution channels«. Singh (2000, 251) folgend, gingen Diffie und Hellman damit eines der Grundprobleme der Kryptographie an, denn, so formuliert er pointiert, »[t]he problem of key distribution has plagued cryptographers throughout history.« Der Einfluss des Aufsatzes von Diffie und Hellman auf die Entwicklung der Kryptographie als Forschungsfeld kann kaum überschätzt werden, legt er doch den Grundstein für die sogenannte *asymmetrische*

Kryptographie,[8] die damit von der sogenannten *symmetrischen* Kryptographie abgegrenzt werden kann, und darüber hinaus formativ ist für das, was Katz und Lindell als *moderne Kryptographie* definieren.[9] Wie die Unterscheidung von symmetrischer und asymmetrischer Kryptographie möglich wurde, wird im Folgenden nach einem Überblick über die Grundbegriffe des Feldes anhand von zwei – im doppelten Sinne des Wortes zu verstehenden – Schlüsselproblemen der Kryptographie entfaltet werden: Erstens anhand der Trennung von Schlüssel und Verschlüsselungsverfahren, die als das *Kerckhoffs'sche Prinzip* kanonisch geworden ist, und zweitens anhand der Lösung des Problems der Schlüsselverteilung durch asymmetrische Kryptographie.

2.4.1 Grundbegriffe der Kryptographie

Schematisch betrachtet, besteht ein Verschlüsselungsverfahren aus mehreren Elementen: Einer zu verschlüsselnden Nachricht im Klartext (*Plaintext*), einer Verschlüsselungsmethode, d.h. ein Algorithmus,[10] und einem Schlüssel, der

---

8 Wie zu Anfang des Kapitels bemerkt, riskiert eine Geschichte der Kryptographie aufgrund der mit ihr verbundenen Geheimhaltungspraktiken, nicht alle Ereignisse und Akteur_innen zu kennen. Ein Beispiel dafür ist die Geschichte der asymmetrischen Kryptographie, die – nach heutigem Kenntnisstand – zweimal erfunden wurde: Das erste Mal Ende der 1960er/Anfang der 1970er Jahre durch James Ellis, Clifford Cocks und Malcolm Williamson. Da die drei zum damaligen Zeitpunkt Angestellte des britischen Geheimdienstes GCHQ waren, blieb ihre Erfindung bis zum Ende des 20. Jahrhunderts geheim. Singh (2000, xvii, 279–280) verweist darauf, dass die entsprechenden Informationen erst kurz vor der Publikation seines Buches freigegeben wurden, und auch seine Wiedergabe der Ereignisse ist gekennzeichnet von weißen Flecken, da noch nicht alle Teile dieser Geschichte für die Öffentlichkeit frei zugänglich sind (vgl. ebd., 284). Ein zweites Mal wurde asymmetrische Kryptographie nur kurze Zeit später von Whitfield Diffie und Martin Hellman erfunden – diesmal im Licht der Öffentlichkeit. Aufgrund der besseren Quellenlage wird im weiteren Verlauf ausschließlich auf Diffie und Hellmans Arbeit Bezug genommen.

9 Aus Gründen der Verständlichkeit wird in der vorliegenden Untersuchung nicht diskutiert, welche Neuerungen auf dem Gebiet symmetrischer Kryptographie für die *moderne Kryptographie* grundlegend sind. Weiterführend dazu siehe Shafi Goldwasser und Silvio Micali (1984; 1982).

10 Ein Algorithmus lässt sich basal als eine präzise definierte Abfolge von Handlungsschritten verstehen. Ein Alltagsbeispiel wäre das Befolgen eines Kochrezepts: Alle Zutaten müssen in der richtigen Menge und zum richtigen Zeitpunkt für die korrekte Dauer in den Topf gegeben werden. Je nachdem, an wen oder was ein Algorithmus sich richtet, sind unterschiedliche Grade an Präzision notwendig: Während Menschen

die Details der Verschlüsselung bestimmt (vgl. Singh 2000, 11). Anhand eines einfachen Beispiels lässt sich dies veranschaulichen: Eine Nachricht soll verschlüsselt werden. Die gewählte Verschlüsselungsmethode ist die Cäsar-Chiffre *(Caesar shift cipher)*,[11] die darin besteht, alle Buchstaben des Plaintext[12] um eine bestimmte Anzahl an Stellen im Alphabet zu verschieben und den Plaintext so in einen verschlüsselten *Ciphertext* zu verwandeln. Der Schlüssel bestimmt die Anzahl der Stellen, um die die Buchstaben verschoben werden, sowie die Richtung der Verschiebung. Bei der Cäsar-Chiffre werden alle Buchstaben des Plaintext um drei Stellen nach hinten verschoben, sodass a durch D, b durch E, c durch F ersetzt wird und so fort. Bolters und Grusins Konzept der Remediatisierung folgend lässt sich an dieser Stelle der Verschlüsselungsvorgang als Remediatisierungsvorgang beschreiben, und ein Ciphertext damit als remediatisierter Plaintext.

Die Cäsar-Chiffre ist verhältnismäßig leicht zu brechen: Wird eine solche verschlüsselte Nachricht abgefangen, und ist das verwendete Verfahren bekannt, so müssen bei einem Alphabet mit 26 Buchstaben maximal 25 Kombinationen ausprobiert werden, bis der Ciphertext wieder in den Plaintext verwandelt werden kann. Eine ähnliche Verschlüsselungsmethode aus dem Bereich der monoalphabetischen Substitutionschiffren, bei der im Unterschied zur *shift cipher* die Reihenfolge des Alphabets nicht gewahrt bleiben muss, und die Buchstaben des Plaintext im Ciphertext durch beliebige andere Buchstaben des Alphabets ersetzt werden (einzige Bedingung: die Ersetzung darf innerhalb eines jeweiligen Textes nicht changieren), ist schon wesentlich schwerer zu entschlüsseln: Selbst wenn bekannt ist, dass es sich um eine Substitutionschiffre handelt, so bedeutet dies bei einem Alphabet mit 26 Buchstaben 26! (lies: »26 Fakultät«) Kombinationsmöglichkeiten –

---

in der Regel mit unpräzisen Algorithmen umgehen können (auch angesichts fehlender Zutaten oder einer etwas zu hohen Temperatur können sie ein Gericht fertigkochen), sind Computer nicht dazu in der Lage, eine ungenau formulierte Handlungsanweisung auszuführen (vgl. Cormen 2013, 1).

11 Tatsächlich ist diese Chiffre nach ihrem prominentesten Nutzer und Erfinder, Julius Cäsar, benannt (vgl. Singh 2000, 9–10) und fällt in die Kategorie der monoalphabetischen Substitutionschiffren. Chiffrieren bezieht sich auf das Austauschen einzelner Buchstaben, während codieren das Austauschen ganzer Wörter bezeichnet (vgl. ebd., 30).

12 Der zu verschlüsselnde Plaintext wird im Folgenden stets klein geschrieben, der verschlüsselte Ciphertext hingegen in Großbuchstaben.

ausgeschrieben sind das über 400.000.000.000.000.000.000.000.000 Kombinationsmöglichkeiten (vgl. ebd.). Nun könnte man darauf schließen, dass daraus zu folgen habe, dass es größeren Schutz vor Entschlüsselung böte, das verwendete Verfahren geheim zu halten, doch dem ist nicht so.[13] Das sture Durchprobieren von Kombinationen scheidet angesichts von 26! Kombinationsmöglichkeiten (vor allem, ohne auf Computer zurückgreifen zu können) zwar als Entschlüsselungsmethode aus, wodurch die monoalphabetische Substitutionschiffre in der westlichen Welt lange für absolut sicher gehalten wurde. Doch zufälliges Ausprobieren von Möglichkeiten ist nicht die einzige Methode der Kryptanalyse, die auf einen Ciphertext anwendbar ist. Der arabische Gelehrte Abū Ya'qūb ibn Ishāq al-Kindī erfand ca. im 9. Jahrhundert[14] ein kryptanalytisches Verfahren, das heute unter dem Namen *Frequenzanalyse* bekannt ist, und dessen Grundprinzip darin besteht, Annahmen über den Plaintext zu treffen, die zu dessen Entschlüsselung dienlich sein könnten. Al-Kindīs Methode besteht darin, die Vorkommnisse der Buchstaben (oder Symbole) eines Ciphertexts zu zählen. Der Buchstabe, der am häufigsten vorkommt, muss dem Buchstaben entsprechen, der in der Sprache des Plaintexts statistisch gesehen am häufigsten verwendet wird (vgl. ebd., 17–19). Ist der Plaintext auf Deutsch verfasst, entspräche dies einem e, das mit ca. 17 % der am häufigsten verwendete Buchstabe des Alphabets ist, gefolgt von dem Buchstaben n mit einer Häufigkeit von ca. 10 % (vgl. Paar/Pelzl 2016, 9). Al-Kindī weist ebenfalls darauf hin, dass Texte auch in ihrem Ausdruck und ihrer Form gewissen Regelhaftigkeiten gehorchen, d.h. dass sie beispielsweise je nach Textgattung mit einer bestimmten Formulierung beginnen, was für die Entschlüsselung hilfreich sein kann (vgl. Mrayati et al. 2003, 82). Je länger ein Ciphertext ist, desto besser funktioniert diese Methode, vorausgesetzt, dass er nicht in verschiedenen Sprachen verfasst ist, die Rechtschreibregeln eingehalten, sowie keine gezielten Maßnahmen ergriffen wurden, um eine Frequenzanalyse zu umgehen, wie beispielsweise Wörter, die den Buchstaben e enthalten, komplett zu vermeiden (vgl. Singh 2000, 19–20).

---

13 Der Versuch, Sicherheit durch die Geheimhaltung des Verfahrens zu erzielen, wird als *security by obscurity* bezeichnet und generell als untauglich angesehen (vgl. Paar/Pelzl 2016, 12).

14 Al-Kindīs Manuskript wurde erst im Jahr 1987 wiederentdeckt, das genaue Datum der Publikation ist unbekannt (vgl. Singh 2000, 17). 2003 erschien erstmals eine englischsprachige und kommentierte Übersetzung von al-Kindīs Manuskript (vgl. Mrayati et al. 2003).

Europa sollte erst einige Jahrhunderte nach al-Kindīs Erfindung von der Frequenzanalyse erfahren: Im Mittelalter befassten sich hauptsächlich Mönche mit Kryptographie, oder vielmehr mit Kryptanalyse, als sie Teile des Alten Testaments dechiffrierten, die mit der hebräischen Substitutionschiffre *Atbasch*[15] verschlüsselt waren, und auch neue Chiffren erfanden (vgl. ebd., 26). Sukzessive fand die Kryptographie ihren Weg aus den Klöstern hinaus, und wurde im 14. Jahrhundert in Wissenschaft und Alchemie verwendet (vgl. ebd., 27). Im 15. Jahrhundert, beflügelt durch die Wiederbelebung der Künste und Wissenschaften in der Renaissance, sowie dem dazugehörigen politischen Klima, in dem viele unabhängige Stadtstaaten sich gegenseitig Diplomaten sandten, wurde Kryptographie in der westlichen Welt zu einer »burgeoning industry« (ebd.). Gleichzeitig erfuhr auch die Kryptanalyse verstärkte Aufmerksamkeit. Singh (ebd., 27–28) weist darauf hin, dass es zwar möglich sei, dass die Frequenzanalyse in Europa unabhängig von al-Kindīs Methode erfunden wurde, schätzt es aber als ebenso wahrscheinlich ein, dass das Wissen aus der arabischen Kultur übernommen wurde. Während in den folgenden Jahrhunderten zwar immer neue Verschlüsselungsverfahren erfunden wurden (beispielsweise der Nomenklator oder die Vignère-Chiffre), so war doch mit der Brechung der monoalphabetischen Substitutionschiffre durch die Methode der Frequenzanalyse deutlich geworden, dass eine Verschlüsselung auch gebrochen werden kann, ohne dass der Entschlüsselungsalgorithmus einer Umkehrung des Verschlüsselungsalgorithmus folgt, wenn vom Plaintext Rückschlüsse auf den Ciphertext gezogen werden können. Die Unabhängigkeit der Kryptanalyse von den intendierten Verfahren zur Entschlüsselung, sowie ihre generelle Bedeutung für die Erfindung neuer kryptographischer Verfahren sollte sich in den folgenden Jahrhunderten mit weiteren Schwerpunkten fortsetzen.

2.4.2 Erstes Schlüsselproblem: Das Kerckhoffs'sche Prinzip

1883 publizierte der niederländische Linguist Auguste Kerckhoffs den für das Feld der modernen Kryptographie kanonisch gewordenen Text *La Cryptographie Militaire*.[16] Kerckhoffs (1883, 8) stellt sechs Prinzipien vor, denen militäri-

---

15 Die Atbasch-Chiffre ersetzt den ersten Buchstaben des Alphabets durch den letzten, den zweiten durch den vorletzten etc. (vgl. Singh 2000, 26).

16 Kerckhoffs ist außer für dieses kanonische Werk bekannt für seine Begeisterung für und seine Verdienste um die artifizielle Sprache *Volapük*, und hat nach dem Erscheinen von *La Cryptographie Militaire* extensiv zu dieser publiziert, bis er sich mit Johann Martin Schleyer, dem Erfinder von Volapük, über die Ausrichtung der Kunstsprache

sche Kryptographie zu folgen habe, und leitet diese mit einer Unterscheidung von verschlüsselter brieflicher Kommunikation zwischen Einzelpersonen und verschlüsselter militärischer Kommunikation per Telegraphie, beispielsweise zwischen Befehlshabern einer Armee, ein:

> »Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux.«[17]

Über diesen Satz schreibt Kahn (1967, 234): »This clear recognition of the new order constitutes Kerckhoffs' first great contribution to cryptology.« Was Kahn als »new order« bezeichnet, worauf er aber nicht konkreter eingeht, ist der von Kerckhoffs ebenfalls nur flüchtig erwähnte, aber doch als signifikant bestimmte Medienwechsel vom Brief zur Telegraphie. Ungefähr hundert Jahre vor dem Erschienen von *La Cryptographie Militaire* begann in Frankreich der Ausbau des optischen Telegraphennetzes (vgl. Flichy 1994, 55). Mit diesem neuen Medium veränderte sich die Übertragungsgeschwindigkeit von Nachrichten: Verdoppelte sich gegen Ende des 19. Jahrhunderts bereits durch den Ausbau des Straßennetzes die Transportgeschwindigkeit von Briefen, so amplifizierte die optische Telegraphie diesen Prozess um ein Vielfaches, und die Übertragung einer Nachricht von Paris nach Valenciennes (ca. 190 km Luftlinie) dauerte nur noch ca. 15 Minuten (vgl. ebd.). Doch mit der optischen Telegraphie kam noch eine weitere Neuerung: Die Notwendigkeit, die übertragenen Nachrichten mittels eines standardisierten Verfahrens zu kodieren. Dies sicherte die Geheimhaltung der übermittelten Nachrichten, und beschleunigte darüber hinaus die Nachrichtenübertragung noch weiter (vgl. ebd., 58). In der ersten Hälfte des 19. Jahrhunderts schritt die Entwicklung der elektrischen Telegraphie voran, die abermals eine starke Erhöhung der Übertragungsgeschwindigkeit zur Folge hatte. Im »für die Entstehung des optischen wie auch des elektrischen Telegraphen charakteristische[n]

überwarf: Während Schleyer Volapük zu einer möglichst umfassenden Form bringen wollte, die zugleich ihre Künstlichkeit verschleiern sollte, wollte Kerckhoffs die Sprache verschlanken und vereinfachen (vgl. Kahn 1967, 232; Andreas 2014, 160).

17 »Es sollte zwischen einem Chiffriersystem, das für einen momentanen Briefwechsel zwischen einigen wenigen isolierten Personen gedacht ist, und einer Methode der Kryptographie, die dazu bestimmt ist, auf unbegrenzte Zeit die Korrespondenz verschiedener Heerführer untereinander zu regeln, unterschieden werden.« Übersetzung MS.

Anspruch, ein weltumspannendes Netz zu errichten« (ebd., 72), lag auch die Notwendigkeit für die Standardisierung des Systems, sowie der zu übertragenden Daten, sodass Mitte des 19. Jahrhunderts das Morse-Alphabet für die Chiffrierung[18] der zu übertragenden Nachrichten verwendet wurde. Doch zurück zu Kerckhoffs: Im Falle von telegraphiegestützter militärischer Kommunikation, so bemerkt dieser, gebe es zwei Dinge, die besondere Beachtung finden müssen. Zum einen sei es nicht möglich, die Vereinbarungen der verschlüsselten Kommunikation, d.h. die Verschlüsselungsmethode, spontan nach Belieben zu ändern. (Dies wäre unter Umständen zwischen zwei per Brief kommunizierenden Parteien möglich, jedoch nicht innerhalb eines Systems, in dem eine Person konstant mit vielen anderen kommuniziert.) Zum anderen müsse man damit rechnen, dass Soldaten gefangen genommen würden; daher dürften diese keine Informationen bei sich tragen, die den Feinden das Brechen der verwendeten Verschlüsselung erleichtern könnten (vgl. Kerckhoffs 1883, 8). Basierend auf diesen beiden Einschränkungen formuliert Kerckhoffs (ebd.) sechs Prinzipien militärischer Kryptographie:

1. Ein kryptographisches System sollte, wenn auch nicht theoretisch, dann wenigstens praktisch nicht zu brechen sein;
2. ein kompromittiertes System sollte keine Gefahr für die kommunizierenden Parteien darstellen;
3. der Schlüssel sollte einfach memorierbar sein (spezifisch: ohne dass er notiert werden muss), sowie einfach auszutauschen;
4. die verschlüsselte Nachricht muss telegraphisch übertragbar sein;
5. die Verschlüsselungsmethode sowie die dazugehörigen Dokumente sollten portabel sowie von einer Person allein verwendbar sein;
6. das kryptographische System sollte einfach zu bedienen sein und nicht viel Vorkenntnisse erfordern.

Kahn (1967, 235) evaluiert: »[A]ny modern cryptographer would be very happy if any cipher fulfilled all six. Of course, it has never been possible to do that.« Dies führt Kahn darauf zurück, dass die Forderungen zueinander inkompatibel seien, und schreibt weiter, dass in der Regel die erste Forderung geopfert werde. (Dies wird sich wenige Jahre nach Kahns Publikation verändert haben,

18 Gemeinhin wird von *Morse-Code* gesprochen, doch mit Singhs (2000, 30) Distinktion von Chiffrieren (Austausch einzelner Buchstaben) und Codieren (Austausch ganzer Wörter) muss hier korrekterweise von Morse-Chiffrierung gesprochen werden.

doch dazu später mehr.) Die erste Forderung ist jedoch, so könnte man sagen, der Grundgedanke der Kryptographie: Kerckhoffs beweist an dieser Stelle sein Wissen um die Frequenzanalyse, mittels derer die monoalphabetische Substitutionschiffre, die theoretisch nicht zu brechen schien, praktisch dennoch zu entschlüsseln war – ein Szenario, das sich bestenfalls nicht wiederholen sollte. Die fünfte und sechste Forderung Kerckhoffs nach Portabilität sowie Einfachheit in der Verwendung lassen sich mit heutigem Vokabular als Forderungen nach Usability beschrieben, und zeugen von Kerckhoffs' Umsichtigkeit.[19] Nicht ganz so selbsterklärend sind die zweite bis vierte Forderung, auf die an dieser Stelle genauer eingegangen werden soll.

Die vierte Forderung, dass die verschlüsselte Nachricht telegraphisch übertragbar bleiben muss, ist ein medienspezifisches Argument, das quer zu der Geschichte der Kryptographie verläuft, und ein Umdenken erforderlich macht: Historisch betrachtet war Kryptographie, da sie mit der Verschlüsselung von Plaintext befasst ist, notwendigerweise am Medium Schrift orientiert. Darüber hinaus waren allerdings oftmals auch die jeweiligen Trägermedien einer Nachricht von Bedeutung für das verwendete kryptographische Verfahren. Dies lässt sich anhand der auf das fünfte Jahrhundert v. Chr. datierten *Skytale* verdeutlichen, dem ältesten bekannten Gerät, das für militärische Kryptographie eingesetzt wurde. Die Skytale ist ein hölzerner Stab, der eng mit einem dünnen Streifen Pergament oder Leder umwickelt wurde. Die Nachricht wurde längs auf den umwickelten Stab geschrieben, und anschließend wurde der Lederstreifen abgewickelt und zum_zur Empfänger_in transportiert. Auf dem abgewickelten Lederstreifen ist lediglich eine scheinbar zufällige Aneinanderreihung von Buchstaben sichtbar. Um die Nachricht zu entschlüsseln, muss sie erneut auf einen Stab desselben Durchmessers aufgewickelt werden (vgl. Singh 2000, 8–9). Die Integrität des physischen Trägermediums, also von Stab und Lederstreifen, ist von

19 Ab Mitte der 1970er Jahre formierte sich unter dem Namen *Usable Privacy and Security* ein Teilbereich der IT-Sicherheitsforschung, der sich explizit mit der Usability kryptographischer Anwendungen befasst. Zentrales Anliegen von *Usable Privacy and Security* ist die Vereinfachung der Anwendung kryptographischer Verfahren, sodass User_innen diese tatsächlich verwenden (können), und nicht aus Unkenntnis oder Bequemlichkeit umgehen (vgl. Garfinkel/Lipford 2014). Kennzeichnend für diesen Ansatz ist die Rehabilitierung von User_innen, die nicht mehr als (zusätzliches) Sicherheitsproblem betrachtet werden sollen, und die Verlagerung der Verantwortung für die (korrekte) Anwendung von Sicherheitsmechanismen auf Designer_innen (vgl. Adams/Sasse 1999).

elementarer Bedeutung: Verändert sich der Abstand zwischen den Buchstaben, oder wird ein dickerer oder dünnerer Stab verwendet, so lässt sich die Nachricht nicht mehr entschlüsseln. Obgleich dieses Beispiel sehr alt ist, so waren kryptographische Methoden, die auf den physischen Eigenschaften ihrer Trägermedien basierten, auch noch zu Kerckhoffs' Zeit im Einsatz. Ein Beispiel dafür ist die Fleissner-Scheibe,[20] die, ebenso wie die Skytale, das kryptographische Prinzip der Transposition verwendet, bei der der Plaintext nicht durch die Substitution einzelner Buchstaben, sondern durch deren Anordnung in einen Ciphertext verwandelt wird (vgl. Bauer 1997, 93). Die Fleissner-Scheibe ist eine metallene quadratische Scheibe mit quadratischen Aussparungen, in die jeweils einzelne Buchstaben eines Plaintexts geschrieben werden. Sind alle Felder voll, so wird die Scheibe um 90 Grad gedreht, und erneut wird weitergeschrieben, bis alle Felder ausgefüllt sind. Nach insgesamt vier Durchgängen ist ein quadratisch angeordneter Buchstabenblock entstanden, der am Stück gelesen keinen Sinn ergibt, aber durch die Linse des Drehrasters seine Nachricht offenbart.[21] Auch hier ist die Form/atierung der Nachricht, die kennzeichnend für die Medialität des kryptographischen Verfahrens ist, für die Ver- und Entschlüsselung entscheidend. Ähnlich wie bei dem Transport des Lederriemens der Skytale wird auch die Form des mittels Fleissner-Scheibe verschlüsselten Textblocks während des Transports gewahrt. Erführe die verschlüsselte Nachricht durch den Transport eine Remediatisierung, so müsste für die Entschlüsselung dieser eine Anleitung beiliegen, um den bei dem_der Empfänger_in angekommenen Nachrichteninhalt erneut in die mediale Ausgangsform zu überführen, da diese Teil der Verschlüsselung ist. Dies wäre, vor allem in einer Kriegssituation aufgrund des zeitlichen Mehraufwands und einer erhöhten Fehleranfälligkeit nicht praktikabel. Die Forderung nach telegraphischer Übertragbarkeit, mit der die

---

20 Bauer (1997, 95) weist darauf hin, dass diese Verschlüsselungsmethode bereits im Jahr 1745 nachgewiesen werden konnte, aber aus Unkenntnis des genauen Ursprungs dem österreichischen Oberst Eduard Fleissner zugeschrieben wird, der diese Methode in seinem 1881 verlegten *Handbuch der Kryptographie* erläutert.

21 An dieser Stelle wird die Nähe der Fleissner-Scheibe zu steganographischen Verfahren deutlich, wie beispielsweise zu der auf den italienischen Philosophen und Mathematiker Gerolamo Cardano zurückgehenden Raster-Methode. Cardanos Methode basierte darauf, eine mittels einer Schablone angeordnete Nachricht mit weiterem Text (beispielsweise einem Gedicht) zu umgeben, um ihre Existenz zu verschleiern. Nur wer eine passgenaue Schablone anlegt, kann die versteckte Nachricht sehen (vgl. Bauer 1997, 23–24).

Trennung von Verschlüsselungsleistung und Form/atierung einhergeht, ist also ein Argument über die Medialität von Kryptographie.

Auch Kerckhoffs zweite Forderung ist voraussetzungsreich: Wie kann ein kompromittiertes System kein Problem für verschlüsselte Kommunikation, also geheimzuhaltende Inhalte sein? Kerckhoffs (1883, 9–10) führt aus:

> »Quant à la nécessité du secret, qui, à mes yeux, constitue le principal défaut de tous nos systèmes de cryptographie, je ferai observer qu'elle restreint en quelque sorte l'emploi de la correspondance chiffrée aux seuls commandants en chef. Et ici j'entends par secret, non la clef proprement dite, mais ce qui constitue la partie matérielle du système : tableaux, dictionnaires ou appareils mécaniques quelconques qui doivent en permettre l'application. En effet, il n'est pas nécessaire de se créer des fantômes imaginaires et de mettre en suspicion l'incorruptibilité des employés ou agents subalternes, pour comprendre que, si un système exigeant le secret se trouvait entre les mains d'un trop grand nombre d'individus, il pourrait être compromis à chaque engagement auquel l'un ou l'autre d'entre eux prendrait part. Rien qu'à ce point de vue il y aurait lieu de condamner l'emploi du dictionnaire chiffré, qui est en usage aujourd'hui dans l'armée.«[22]

Mit dem *système* sind also alle Bestandteile eines kryptographischen Systems gemeint außer dem Schlüssel selbst: Tabellen (wie sie beispielsweise für Substitutionschiffren verwendet werden), Kodierungswörterbücher (gegen die Kerckhoffs sich im Besonderen ausspricht), oder mechanische Geräte (wie beispielsweise die Fleissner-Scheibe). Kerckhoffs ist aus rein praktischer Perspektive beizupflichten: Je mehr Glieder die Kette von Ver- und Entschlüsselung hat, je mehr Materialien geheim zu halten, und je mehr Menschen

22 »Was die Notwendigkeit der Geheimhaltung angeht, die in meinen Augen das größte Manko all unserer kryptographischen Systeme ist, möchte ich darauf hinweisen, dass sie die Verwendung verschlüsselter Korrespondenz in gewisser Weise auf die Oberbefehlshaber beschränkt. Und hier meine ich mit Geheimhaltung nicht den Schlüssel selbst, sondern das, was den materiellen Teil des Systems ausmacht: Tabellen, Wörterbücher oder mechanische Geräte, die die Verwendung des Schlüssels ermöglichen. In der Tat ist es nicht notwendig, imaginäre Geister zu erschaffen und die Unbestechlichkeit untergeordneter Mitarbeiter oder Agenten in Frage zu stellen, um zu verstehen, dass ein System, das Geheimhaltung erfordert, und in den Händen zu vieler Individuen liegt, bei jedem Einsatz, an dem einer von ihnen teilnimmt, kompromittiert werden könnte. Allein unter diesem Gesichtspunkt ist die Verwendung des verschlüsselten Wörterbuchs, wie es heute im Militär im Einsatz ist, zu verurteilen.« Übersetzung MS.

an diesem Prozess beteiligt sind, desto mehr Schwachstellen hat diese Kette auch. Diese Erkenntnis resultiert für Kerckhoffs jedoch nicht darin, alle Materialien und Menschen aus dieser Kette auszuschließen, wobei er schon auf eine Reduktion drängt (siehe Forderung 5), sondern darin, erstmals in der Geschichte der Kryptographie das kryptographische System, die Verschlüsselungsmethode, explizit vom Schlüssel zu trennen (vgl. Kahn 1967, 235), verbunden mit dem Anspruch, dass die Bekanntheit des kryptographischen Verfahrens nicht dazu führen dürfe, dass die Verschlüsselung gebrochen sei. Dies schließt bestimmte kryptographische Verfahren aus, wie beispielsweise Code-Wörterbücher oder auch Fleissner-Scheiben, da die Trennung von Verfahren und Schlüssel bei diesen nicht gegeben ist. Zusammengenommen mit der dritten Forderung danach, dass der Schlüssel so leicht zu merken sein müsse, dass er nicht notiert werden muss (wodurch er erneut Teil des *système* werden würde), bilden diese Forderungen den Kern dessen, was heute als Kerckhoffs'sches Prinzip kanonisch geworden ist, und dessen zeitgenössische Formulierung folgendermaßen lautet:

> »Ein [sic!] kryptografische Lösung muss auch dann noch sicher sein, wenn der Angreifer alle Details des Kryptosystems kennt, mit der Ausnahme des Schlüssels. Insbesondere muss das Verfahren auch dann sicher sein, wenn dem Angreifer der Ver- und Entschlüsselungsalgorithmus bekannt sind.« (Paar/Pelzl 2016, 12)

Die Essenz des Kerckhoffs'schen Prinzips ist damit nichts Geringeres als eine doppelte Modularisierung der Kryptographie: Einerseits durch die Trennung von Verfahren und Schlüssel, andererseits durch die Trennung von Verschlüsselung und Form. Mit Krämer (2003, 82) lässt sich an dieser Stelle von der erkenntnisinteressenabhängigen Unterscheidung von Form und Medium Gebrauch machen: Verschlüsselung als Medium nach Kerckhoffs wird getrennt von einer spezifischen Form, insofern diese Form nicht mehr Teil der Verschlüsselungsleistung sein darf, und zugunsten einer scheinbaren Formlosigkeit vernachlässigt werden muss. Diese beiden Modularisierungen konstituieren sich wechselseitig, da sich nicht argumentieren lässt, welche die jeweils andere bedingt. Die Verwendung einer kryptographischen Methode wie beispielsweise der Transposition, die nah an der Steganographie liegt, und bei der die Form, oder vielmehr die Formatierung des Ciphertexts Teil der Verschlüsselungsleistung und damit der Remediatisierung des Plaintexts ist, fällt damit kategorisch aus. Kerckhoffs' Forderung, die elektronische Telegraphie solle der standardisierte Übertragungsweg militärischer

Kryptographie sein, argumentiert so für grundsätzliche und barrierearme Remediatisierbarkeit verschlüsselter militärischer Kommunikation über den Remediatisierungsvorgang der Verschlüsselung hinaus. Der Medienwechsel – und damit auch Materialitätswechsel – verschlüsselter Kommunikation von Schrift auf Papier zu elektronischen Signalen und wieder zurück soll Teil militärischer Kryptographie werden. Dies kann nur durch eine Regulierung der Medialität von Kryptographie selbst gelingen: Der Vernachlässigung einer spezifischen Anordnung, Form und Materialität des Ciphertexts als Ergebnis der Verschlüsselung zugunsten einer Verschlüsselungsmethode, deren Remediatisierung des Plaintexts sich ausschließlich auf eine basale Variante des Mediums Schrift bezieht und in diesem verbleibt, und deren Ergebnis daher erneut durch die Telegraphie remediatisiert werden kann, ohne an Sicherheit zu verlieren.

Die Geschichte der Kryptologie ist jedoch, wie Mediengeschichte so oft, keine lineare Fortschrittsgeschichte: So wurden die von Kerckhoffs formulierten Forderungen bereits im Zweiten Weltkrieg von den Deutschen nicht konsequent beachtet. Die Verwendung der Chiffriermaschine Enigma war, wie Friedrich Bauer und Dominik Landwehr ausführen, von einigen »Dummheiten der Deutschen« (Bauer 1997, 200), oder anders formuliert: durch »[s]ystematische und wiederholt begangene Fehler auf der Seite Deutschlands und der Achsenmächte« (Landwehr 2008, 49) geprägt, was schlussendlich zu der erfolgreichen Kryptanalyse seitens der Briten führte. Da Landwehr in *Mythos Enigma. Die Chiffriermaschine als Sammler- und Medienobjekt* vor allem auf die Automatisierung von Ver- und Entschlüsselung eingeht und darlegt, wie durch die kryptanalytischen Unternehmungen der Polen und schließlich der Briten in Bletchley Park die Mathematik zur »Königsdisziplin in der Kryptografie, respektive in der Kryptoanalyse« (ebd., 57) avancierte, werde ich an dieser Stelle auf eine detaillierte Wiedergabe dieser Ereignisse verzichten. Stattdessen möchte ich als kurze Ergänzung zu Landwehrs ansonsten sehr ausführlichen Untersuchung einen Aspekt beleuchten, den Landwehr ausgespart hat, und kursorisch darlegen, inwiefern die Verwendung der Chiffriermaschine Enigma den Kerckhoffs'schen Forderungen widersprach. Auf die Ähnlichkeit der Enigma zur Schreibmaschine ist bereits Friedrich Kittler ausführlich eingegangen. Kittler (1986, 364) bemerkt, die Enigma habe mit ihrer »Maschinenmathematik Kryptographen von ihrer Handarbeit« erlöst – und während das für die Kryptograph_innen sicher stimmt, so gilt es nicht für alle am Prozess der Entschlüsselung beteiligten Personen. Die Enigma konnte im Gegensatz zur Schreibmaschine kein Papier bedrucken, was dazu

führte, dass für eine schnelle Verwendung drei Personen notwendig waren, »one to read the incoming text and press the keys, one to call out the letters in a loud voice as they lit up, one to write down the text« (Kahn 1967, 422), womit bereits der fünften Forderung Kerckhoffs widersprochen wurde. Auch die dritte Forderung, der Schlüssel solle einfach memorierbar sein, wurde nicht eingelöst – dies lag auch daran, dass die Deutschen, um die Sicherheit der Verschlüsselung zu erhöhen, drei verschiedene Schlüssel verwendeten, die täglich ausgetauscht wurden, was es notwendig machte, sie in Codebüchern aufzuschreiben (vgl. Singh 2000, 146–147) – so wurden die Schlüssel Teil des *systèmes*. Den Briten gelang es Anfang der 1940er Jahre sowohl einige funktionstüchtige Enigmas sowie Benutzungsvorschriften und das sog. *Kurzsignalhandbuch* aus angegriffenen Schiffen und U-Booten zu bergen, die wichtige Informationen für die Kryptanalyse lieferten (vgl. Bauer 1997, 202–203). So brach die Enigma mit Kerckhoffs' zweiter Forderung, indem das Bekanntwerden des Systems die Verschlüsselung kompromittierte. Die unklare Abgrenzung von Schlüssel und System betraf noch einen weiteren Aspekt: Da die in der Enigma verbauten Walzen nicht ausgetauscht, sondern erst gegen Ende des Zweiten Weltkriegs in manchen militärischen Abteilungen um eine Walze ergänzt wurden, wurden die Walzen praktisch zum Teil des Schlüssels, und die strikte Trennung von Verfahren und Schlüssel war damit in zweifacher Weise nicht mehr gegeben.

2.4.3 Zweites Schlüsselproblem: Asymmetrische Kryptographie

In der Geschichte der Kryptographie lassen sich, so die eingangs formulierte These, im doppelten Sinne des Wortes zwei Schlüsselprobleme ausmachen. Das erste betrifft die Trennung von Verschlüsselungsverfahren und Schlüssel. Obwohl diese Trennung bereits in Kapitel 2.3.1 anhand der monoalphabetischen Substitutionschiffren beispielhaft verdeutlicht werden konnte, woraus hervorgeht, dass die Trennung von Verfahren und Schlüssel in der Geschichte der Kryptographie immer wieder vorkam, wurde diese Trennung erstmals durch Kerckhoffs' *La Cryptographie Militaire* auf der Ebene der Theoriebildung vollzogen. Die Umsetzung des Kerckhoffs'schen Prinzips ist, wie am Beispiel der Enigma deutlich wurde, in der Praxis nicht so leicht wie man vermuten könnte, da sich die Zugehörigkeiten einzelner Elemente zu System oder Schlüssel durch ihren Gebrauch verschieben können.

Das zweite Schlüsselproblem ist das der »key distribution« (Singh 2000, 251), der Schlüsselverteilung. Von einem heutigen Standpunkt aus lassen sich

– zusätzlich zu der durch Katz und Lindell vorgenommenen Einteilung – zwei Grundtypen von Kryptographie ausmachen: »(1) *symmetric* or *secret key* and (2) *asymmetric* or *public key*« (Lloyd/Adams 2011, 683). Ein kryptographisches Verfahren wird als *symmetrisch* bezeichnet, wenn derselbe Schlüssel für die Ver- und Entschlüsselung verwendet wird (vgl. ebd., 683). Ein solches Verfahren setzt voraus, dass Sender_in und Empfänger_in sich auf einen Schlüssel geeinigt haben, und dass beide eine Kopie dieses Schlüssels besitzen müssen (vgl. ebd.). Dem Kerckhoffs'schen Prinzip folgend basiert die Sicherheit eines symmetrischen Verfahrens einzig und allein auf der Geheimhaltung des Schlüssels, weswegen symmetrische Kryptographie auch als *secret key cryptography* bezeichnet wird. Dies bringt in der Praxis ein grundsätzliches Problem mit sich: Da verschlüsselte Kommunikation notwendigerweise medial vermittelt ist, gibt es keine Möglichkeit, sich über den Schlüssel zu verständigen, denn der Übertragungsweg wird grundsätzlich als ein »unsicherer Kanal« (Paar/Pelzl 2016, 5) konzeptualisiert. Als unsicher wird ein Kanal nicht etwa deshalb beschrieben, weil dem Übertragungsmedium gewisse Eigenleistungen zugestanden würden, die über die bloße Vermittlung von Inhalten hinausgehen, sondern weil davon ausgegangen wird, dass eine unbefugte, dritte Partei den Inhalt der Kommunikation während der Übertragung abfangen und/oder manipulieren wollen würde – andernfalls wäre die Verschlüsselung des Kommunikationsinhaltes auch nicht notwendig. Eine Möglichkeit für einen sicheren Schlüsselaustausch ist, dass die beiden kommunizierenden Parteien einen anderen Kanal wählen, von dessen Sicherheit sie ausgehen, oder bei einem Treffen in leiblicher Ko-Präsenz einen Schlüssel vereinbaren.[23] Die Ende der 1970er Jahre durch Whitfield Diffie und Martin Hellman erfundene *public key cryptography*, auch *asymmetrische Kryptographie* genannt, nimmt sich genau dieses Umstands an, der durch eine veränderte Medienlage in besonderer Weise in den Vordergrund kryptographischer Fragestellungen rückt.

ARPANET und der Beginn computergestützter Kommunikation

1958 wurde in den USA die *Advanced Research Projects Agency*, kurz: ARPA gegründet, die dem Verteidigungsministerium unterstellt war, und Forschungen in den Bereichen Verhaltenswissenschaft, Materialwissenschaft und Raketenabwehr durchführte (vgl. Abbate 1999, 36). 1962, als Informatik noch kei-

23 Besteht Grund zur Annahme, dass trotz Sicherheitsvorkehrungen ein neuer Schlüssel vereinbart werden muss, so müssen sich beide Parteien erneut treffen.

ne universitäre Disziplin war, wurde das *Information Processing Techniques Office* (IPTO) als ARPA-Untergruppe gegründet, wodurch ARPA die treibende finanzielle Kraft hinter informatischer Forschung wurde (vgl. ebd.). Durch das IPTO entstanden in den folgenden Jahren mehrere Forschungszentren an Universitäten wie dem MIT, der Carnegie Mellon und der UCLA und einigen weiteren, die durch das ARPANET verbunden werden sollten (vgl. ebd.). Im Fokus der Vernetzungsbemühungen stand zunächst das sog. *time share computing*: Zentralrechner waren teuer, und die begrenzten Kapazitäten sollten über das ARPANET auch anderen universitären Standorten zur Verfügung gestellt werden (vgl. Warnke 2011, 30–31). Am 29.10.1969 wurde schließlich das ARPANET eingeweiht, und der erste Nutzungsversuch endete schneller als geplant mit dem berühmt-berüchtigten ersten Wort des Internets, »LO«, da das System zusammenbrach, bevor das Wort »LOGIN« zu Ende geschrieben werden konnte (vgl. ebd., 33). Die in medienwissenschaftlicher Literatur der letzten Jahre meistbesprochene Erfindung im Zusammenhang mit dem ARPANET ist das *Packet Switching*, das gleichzeitig die Grundlage für das Internet legte,[24] doch auch die E-Mail als neue Form der Kommunikation entstand mit dem ARPANET. Entgegen dem ursprünglich angedachten Verwendungszweck des ARPANET stand das Teilen von Rechenressourcen schnell nicht mehr im Vordergrund, im Gegenteil verringerte sich die Nachfrage nach Fernressourcen. Abbate (1999, 104) bemerkt dazu treffend: »Ironically, however, many sites rich in computing resources seemed to be looking in vain for users.« Verschiedene Faktoren zeichnen für diese Entwicklung verantwortlich: Einerseits waren die wenigen verbundenen Universitäten bereits gut mit Computern ausgestattet, was die Nachfrage nach zusätzlichen Ressourcen schmälerte. Darüber hinaus wurden Programme anderer Standorte eher auf die Computer einer jeweiligen Universität kopiert als per Fernzugriff ausgeführt. Auch die antizipierte Nutzung des »distributed computing«, bei dem eine Rechenaufgabe zwischen verschiedenen vernetzten Computern aufgeteilt wird, wurde kaum in Anspruch genommen, da sie an den administrativen Vorgängen innerhalb der Universitäten scheiterte (vgl. ebd., 104–105). Schlussendlich wurde auch im Verlauf der 1970er Jahre Computerhardware günstiger, und die ehemals verwendeten

24 Die Geschichte des ARPANET ist wesentlich detailreicher und komplizierter, als sie hier dargestellt werden soll, da dies nicht im Fokus dieses Buchs steht. Für einen ausführlichen Überblick siehe unter anderem Abbate (1999), sowie Warnke (2011) und Gießmann (2016); speziell zu *Packet Switching* siehe Sprenger (2015).

Mainframe-Computer an den Universitäten durch Mini- oder Microcomputer ersetzt, wodurch das ursprüngliche Problem, dessen Lösung das ARPANET darstellen sollte, auf anderem Wege gelöst wurde (vgl. ebd., 105). Doch mit dem ARPANET bildete sich auch eine neue Form der Kommunikation aus, und nahm die E-Mail als ein Phänomen digitaler Kulturen unvorhergesehen Fahrt auf.

Zu Beginn der 1960er Jahre hatten Nutzer_innen der Time-Sharing-Computer einen eigenen passwortgeschützten Bereich, auf dem Dateien abgelegt werden konnten. Diese Bereiche und die Schaffung von Zugangsvoraussetzungen durch Passwörter lassen sich mit Paul Ferdinand Siegert (2008, 191) als eine erste Form der Herstellung von Sicherheit als *access control*, also der Kontrolle von Zugangsberechtigungen betrachten. Mit der Zeit etablierte sich das Freigeben von Textdateien sowohl für einzelne Nutzer_innen, die anhand ihres Logins identifizierbar waren, als auch über *Public Domains*, die für alle zugänglich waren, als Methode der Kommunikation der Nutzer_innen des Time-Share-Systems untereinander (vgl. ebd.). 1965 wurde im Zuge der Arbeit am Dateisystem des *Compatible Time Share Systems*, kurz CTSS, ein System-Kommando namens »MAIL« entworfen und in CTSS implementiert. MAIL sollte Systemadministrator_innen dazu befähigen, Nutzer_innen über von Backupmedien wiederhergestellte Daten zu informieren. Die Idee Tom Van Vlecks, eines der Entwickler von MAIL, dass mit dem MAIL-Befehl alle Nutzer_innen allen anderen Nutzer_innen desselben Computers zeitversetzt Nachrichten egal welchen textlichen Inhalts zukommen lassen konnten, setzte sich durch, und so wurde MAIL in seiner erweiterten Funktionalität 1965 fester Bestandteil des CTSS-Dateisystems. MAIL war ab diesem Zeitpunkt ein *Push-Dienst* geworden, was, wie Siegert (ebd., 192) feststellt, integraler Bestandteil dessen werden sollte, was heute als E-Mail bezeichnet wird. Zu diesem Zeitpunkt operierte MAIL nur innerhalb desselben Computers, doch das sollte sich mit der breiteren Einbindung von MAIL in das ARPANET ändern. Dazu waren, wie Siegert (ebd., 198) ausführt, zwei Herausforderungen zu bewältigen: Es musste ein standardisiertes Protokoll für den Nachrichtenaustausch geschaffen werden, um die verschiedenen Mainframe-Computer miteinander zu verbinden, sowie ein computerübergreifendes Adressenschema entwickelt werden, damit die jeweiligen Nutzer_innen direkt adressierbar waren. Bemerkenswert ist die Tatsache, dass die verschiedenen am ARPANET beteiligten Akteur_innen – beispielsweise das Militär, die universitären Forscher_innen und diverse Firmen – unterschiedliche Ansprüche an Nachrichtenaustauschsysteme hatten, und so »Konferenz-Systeme, Chat-Systeme, schwarze Bretter

u.a.« (Ebd.) miteinander konkurrierten. Das erste funktionstüchtige Mail-Programm, das eine Kommunikation zwischen vernetzten Computern desselben Betriebssystems erlaubte, wurde Anfang der 1970er Jahre von Ray Tomlinson für das Betriebssystem TENEX geschrieben (vgl. Abbate 1999, 106). Kurze Zeit später wurde über die Möglichkeiten einer Vereinheitlichung der Mailsysteme von Time-Sharing-Betriebssystemen diskutiert, und wie diese zwischen vernetzten Computern zur Anwendung kommen könnten. Trotz der offensichtlichen Beliebtheit von E-Mail-Diensten im Alltag ihrer Nutzungsgemeinde war die Möglichkeit, Nachrichten zu versenden, auf der Ebene der Planung ein Nebenprodukt des ARPANET und wurde in den Papieren und Präsentationen, die sich an die geldgebenden Institutionen richteten, bis Mitte der 1970er Jahre kaum erwähnt (vgl. Siegert 2008, 212). Mehr noch: »[D]ie Betonung dieses Dienstes«, führt Siegert (ebd., 213) aus, hätte »das ARPANET-Projekt politisch gefährden können.« Dies lag hauptsächlich daran, dass das Versenden einfacher Textnachrichten gemessen an dem zur damaligen Zeit hohen ökonomischen und ressourcentechnischen Aufwand unangemessen verschwenderisch anmutete (vgl. ebd.). Und obgleich es nicht das Ziel des ARPANET war, ein neues Kommunikationsnetzwerk zu erschaffen – Abbate (1999, 108) weist darauf hin, dass die Möglichkeit, sich gegenseitig Nachrichten senden zu können, sogar als unwichtige Funktion eines wissenschaftlichen Netzwerks abgetan wurde – wurde durch eine Untersuchung im Jahr 1973 ermittelt, dass Dreiviertel des Netzwerkverkehrs durch E-Mails verursacht wurde. Damit war der ursprünglich anvisierte Einsatzbereich, das Teilen von Dateien und Rechenleistung, eindeutig in den Hintergrund gerückt (vgl. Siegert 2008, 217), und ein »radical shift in the ARPANET's identity and purpose« (Abbate 1999, 109) eingetreten: »The rationale for building the network had focused on providing access to computers rather than to people« (ebd.). Dieser radikale Shift sollte in den nächsten Jahren mit der Entwicklung des Internets weiter voranschreiten.

Eine Kiste mit zwei Schlössern

Die Nutzugspraktiken des ARPANET, die unverhofft die E-Mail als neue Form der Kommunikation hervorbrachten, waren auch für Diffies und Hellmans Überlegungen ausschlaggebend, die die Ablösung des ARPANET aus dem vornehmlich militärischen und akademischen zugunsten eines privatwirtschaftlichen Kontexts antizipierten. So schreiben sie in der Einleitung von *New Directions In Cryptography*:

»The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.« (Diffie/Hellman 1976, 644)

Tatsächlich spielte Verschlüsselung in der Entwicklung des ARPANET, und damit auch für die Entstehung der E-Mail keine Rolle,[25] wodurch die Möglichkeit verschlüsselter Kommunikation erst nachträglich durch die Kryptographie beigesteuert wurde. Ein dringlicheres Problem war zunächst die Standardisierung des Adresssystems von E-Mails. Erste Versuche dazu lassen sich auf den Beginn der 70er Jahre zurückdatieren: Eine erste Liste mit 45 Netzwerkadressen und den dazugehörigen Hostnamen war bereits 1971 zum Download verfügbar (vgl. Siegert 2008, 268). Da es schnell umständlich wurde, dieses Dokument zu pflegen, kam der Vorschlag auf, ein solches Dokument in maschinenlesbarer Form online zu pflegen, das neben Adresse und Name des Hostrechners auch die durch ihn unterstützen Dienste anzeigte. Obwohl die Adresskonvention »mailbox@host.domain« erst 1982 verbindlich festgelegt wurde, entstand mit dem »Directory of Electronic Mail« (ebd., 269) Mitte der 1970er Jahre ein Adressbuch, in dem 134 unterschiedliche Netzwerke mit ihren jeweiligen Adressformen verzeichnet waren.[26] Ein solches Adressbuch machte es möglich, per E-Mail mit Personen in Kontakt zu treten, die man nicht bereits persönlich kannte. Obwohl Diffie und Hellman E-Mail nicht

25 Siegert (2008, 151) sieht dies als Beweis dafür, dass das ARPANET in erster Linie für die Forschung, und nicht für militärische Anwendungen konstruiert wurde: »Was hier entstehen sollte, war ein Forschungsnetz. Militärische Erfordernisse eines stabilen Kommunikationssystems unter Kriegsbedingungen, also besonders hohe Ausfallsicherheit, Verschlüsselung oder Prioritätenmanagement, wie sie Baran ausgearbeitete hatte, wurden nicht übernommen. Insofern ist der Schluss, das ARPANET sei ein militärisches Netz, da es von einer militärischen Behörde finanziert und von Baran entsprechend entworfen wurde, nicht haltbar.«

26 Siegert (2008, 269) weist darauf hin, dass zwischen Mailbox und Hostnamen im ARPANET das @-Zeichen verwendet wurde, in anderen Netzwerken aber auch : und ! gebräuchlich waren.

konkret erwähnen, so lässt sich doch darauf schließen, dass die von ihnen bemängelten »severe inconveniences«, die gleichermaßen die Vorteile des neuen Kommunikationsmediums zunichte machen würden, sich auf die Notwendigkeit des Schlüsselaustauschs beziehen, der mit symmetrischer Verschlüsselung *vor* dem Versenden verschlüsselter E-Mails notwendig wäre. Asymmetrische Verschlüsselung erlaube es hingegen, eine verschlüsselte Konversation »between any two individuals regardless of whether they have ever communicated before« (Diffie/Hellman 1976, 644) zu etablieren, ohne dass vorher ein Schlüsselaustausch über einen sicheren Kanal (der nicht leicht zu finden ist) oder während eines persönlichen Treffens stattfinden muss. Wie ist das möglich?

Die Funktionsweise asymmetrischer Kryptographie wird oft anhand des Beispiels einer verschlossenen Kiste erläutert (vgl. Paar/Pelzl 2016, 176; Singh 2000, 258–259): Person A möchte Person B eine Nachricht zukommen lassen, und legt diese in eine Kiste, die mit einem Vorhängeschloss gesichert ist. Bei symmetrischer Kryptographie müssen nun Person A und B über den gleichen Schlüssel verfügen, um die Kiste abzuschließen und zu öffnen. Asymmetrische Kryptographie hingegen funktioniert analog zu einer Kiste mit zwei Schlössern: Person A schließt die Kiste mit ihrem Vorhängeschloss ab und sendet sie an Person B. Person B kann die Kiste nicht öffnen, da sie den Schlüssel zu Vorhängeschloss A nicht hat, und hängt ihrerseits ein Vorhängeschloss B an, zu dem sie den Schlüssel hat, und sendet die Kiste mit zwei Vorhängeschlössern zurück an Person A. Person A wiederum entfernt ihr Vorhängeschloss A und sendet die Kiste mit nur noch dem Vorhängeschloss B zurück an Person B, die die Kiste nun öffnen und die Nachricht lesen kann. Dieser Vorgang erscheint zunächst umständlich, da die Nachricht mehrmals hin und her gesendet werden muss. Nichtsdestotrotz, schreibt Singh (ebd., 259), »[f]or the first time we have a suggestion that key exchange might not be an inevitable part of cryptography.« Dieses Modell hat nur einen Nachteil: Es funktioniert zwar mit Vorhängeschlössern und einer Kiste, die die Nachricht einkapselt, aber nicht mit kryptographischen Verfahren, die die Nachricht remediatisieren. Würden Person A und B denselben Vorgang nicht mit einer Kiste und Vorhängeschlössern, sondern mit einem Text und beispielsweise einer monoalphabetischen Substitutionschiffre durchführen, so wäre das Endergebnis unlesbar: Person A verschlüsselt den Plaintext mit ihrem Schlüssel A und sendet den *Ciphertext A* an Person B. Person B kann *Ciphertext A* nicht entschlüsseln, und verschlüsselt ihn nun erneut mit ihrem Schlüssel B, und sendet dann den *Ciphertext AB* zurück an Person A – so weit,

so gut. Person A kann allerdings den *Ciphertext AB* nicht mit ihrem Schlüssel A entschlüsseln, da die letzte Substitution mit dem Schlüssel B erfolgt ist. Die Anwendung des umgekehrten Verschlüsselungsalgorithmus mit Schlüssel A führt ganz im Gegenteil zu einer weiteren Verschlüsselung, an dessen Ende der *(Ciphertext AB)A* steht, der dann an Person B zurückgesendet werden würde. Person B würde dies durch eine weitere Bearbeitung mit Schlüssel B in *(Ciphertext AB)AB* verwandeln, aber nicht in den Plaintext. Die korrekte Reihenfolge von Ver- und Entschlüsselung muss also der Maxime »last on, first off« (ebd.) gehorchen. Die Lösung dieses Dilemmas liegt unter anderem darin, dass es sich bei den vorangegangenen Schilderungen lediglich um Modelle handelt, und nicht um die Gegenstände selbst, was auch bedeutet, dass die Einschränkungen der Modelle nicht auf die Gegenstände zutreffen müssen. Mit der grundsätzlichen Idee, dass ein Schlüsselaustausch nicht notwendig sei, um verschlüsselte Nachrichten zu versenden, forschten Diffie und Hellman, zu denen inzwischen Ralph Merkle gestoßen war, bis sie in der Verwendung von Einwegfunktionen[27] in Kombination mit modularer Arithmetik[28] eine Möglichkeit für die Umsetzung ihres Vorhabens entdeckten (vgl. ebd., 260–261). Mit dieser Lösung geht auch die Zweiteilung des Schlüssels

27 Eine gegebene Funktion wird als Einwegfunktion bezeichnet, wenn sie in Polynomialzeit berechnet werden kann, ihre Umkehrung allerdings nicht mehr. Bei einer Einwegfunktion, hier beispielhaft als die Funktion $y=f(x)$ dargestellt, geht man davon aus, dass für jedes x genau ein y berechnet werden kann. Die Funktion ist damit *eineindeutig* und kann in *polynomialer Zeit* berechnet werden (vgl. Spitz et al. 2011, 32). Eine solche Funktion wird beispielsweise verwendet, um von einer Datei x eine Hashsumme y zu erzeugen. Möchte man nun von der Hashsumme aus die dazugehörige Datei errechnen, muss der Rechenvorgang umgekehrt durchgeführt werden – dies wird durch die Notation $x=f_1(y)$ dargestellt. Dies ist zwar theoretisch möglich, aber der Rechenaufwand steigt mit jeder Stelle der Hashsumme exponentiell an (vgl. ebd., 33). Aus praktischer Sicht ist ein solches Zurückrechnen unmöglich, da dies je nach Länge der Hashsumme mehrere Jahrzehnte, Jahrhunderte oder sogar Jahrtausende dauern könnte (vgl. Paar/Pelzl 2016, 177–178). Aufgrund der *praktischen* Unumkehrbarkeit der Funktion wird diese als Einwegfunktion bezeichnet.

28 Bei Modularer Arithmetik wird innerhalb eines begrenzten Zahlenraumes ›in Kreisen‹ gerechnet. Dies lässt sich am besten anhand eines Alltagsbeispiels für die Anwendung modularer Arithmetik verdeutlichen: der Uhrzeit. Wer um 10 Uhr vormittags eine Aufgabe beginnt, die 8 Stunden dauert, wird um 6 Uhr nachmittags fertig sein. 10 + 8 ergibt innerhalb dieses Systems 6, da ab Erreichen der Zahl 12 am Anfang des Zahlenraumes bei der Zahl 1 weitergezählt wird. Die mathematische Notation lautet: $10 + 8 = 6 \; (mod\ 12)$ (lies: »modulo 12«).

in einen privaten und einen öffentlichen Teil einher, die mathematisch so zusammenhängen, dass der öffentliche Schlüssel mittels des privaten über eine Einwegfunktion generiert wird. Die beiden öffentlichen Schlüssel können über einen unsicheren Kanal ausgetauscht werden. Die Einwegfunktion verhindert, dass der private Schlüssel berechnet werden kann, selbst wenn der öffentliche Schlüssel sowie die verwendete Funktion bekannt sind, wodurch bei diesem Verfahren das Kerckhoffs'sche Prinzip auf elegante Weise gewahrt wird. Zwei miteinander kommunizierende Parteien müssen nun nicht mehr einen symmetrischen Schlüssel austauschen, allerdings wird der herkömmliche Schlüssel*austausch* praktisch durch eine Schlüssel*vereinbarung* ersetzt, da eine Einwegfunktion verabredet werden muss, was entweder in einem (Telefon-)Gespräch oder in einem zeitversetzten Mailwechsel geschehen kann (vgl. ebd., 265–267). Damit ist das Problem des Schlüsselaustausch über einen unsicheren Kanal zwar gelöst, aber dennoch »the spontaneity of e-mail« (ebd., 267) nicht völlig ausgeschöpft, da nach wie vor nicht einfach verschlüsselt drauf los geschrieben werden kann. Dazu gesellte sich ein weiteres Problem: Das von Diffie und Hellman entwickelte Verfahren kann nur zur Generierung von Schlüsseln verwendet werden, aber noch nicht für Ver- und Entschlüsselung von Nachrichten (vgl. Schneier 2015, 513). Nur kurze Zeit später legten Ronald Rivest, Adi Shamir und Leonard Adleman (1978) in ihrem Paper *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* eine Verschlüsselungsmethode vor, die der von Diffie und Hellman beschriebenen Einwegfunktion in ihrer Funktionsweise recht ähnlich ist, und ebenfalls von modularer Arithmetik Gebrauch macht. Die Sicherheit des nach den Anfangsbuchstaben der Nachnamen seiner Erfinder benannten RSA-Verschlüsselungsverfahrens liegt in dem Faktorisierungsproblem großer Zahlen (vgl. ebd., 126): Der Schlüssel ist auch hier in eine öffentliche und eine private Komponente aufgeteilt. Für die private Komponente werden zwei Primzahlen p und q ausgewählt, die miteinander multipliziert die Zahl n ergeben. p und q bleiben privat, n hingegen bildet gemeinsam mit einer weiteren, zufällig gewählten Zahl e den öffentlichen Schlüssel (vgl. ebd., 122–123). Während das Produkt n durch die Multiplikation von p und q schnell berechnet ist, so ist für die Zerlegung von n in p und q bis heute kein effizientes Verfahren bekannt, was die Herstellung von n aus der Multiplikation von p und q (nach aktuellem kryptanalytischen Forschungsstand) zu einer Kandidatin für eine Einwegfunktion macht. Je größer p und q, und damit auch n sind, desto länger dauert im Falle eines Angriffs die Primfaktorzerlegung, und desto sicherer ist

das Verfahren.[29] Singh (2000, 279) bemerkt dazu: »It is now routine to encrypt a message with a sufficiently large value of *N* so that all the computers on the planet would need longer than the age of the universe to break the cipher.« Mit dem öffentlichen Schlüssel (*n*, *e*) kann eine Nachricht *m*, die kürzer ist als *n*, verschlüsselt werden. Ist die Nachricht länger, so muss sie in mehrere Teile aufgeteilt werden. Der Ciphertext entsteht in der Rechnung m_e mod *n* (vgl. Schneier 2015, 467).[30]

Digitale Signaturen

Der Austausch verschlüsselter Nachrichten ohne vorherigen Schlüsselaustausch ist nicht die einzige Funktion asymmetrischer Kryptographie. Eine zweite ist die Möglichkeit, digitale Signaturen zu erzeugen – ein Novum in der Verwendung von Kryptographie. Diffie und Hellman (1976, 645) führen diese Funktion am Beispiel von Unterschriften bei Geschäftsvorgängen ein, die in der Zukunft online, und damit papierlos abgewickelt werden sollen:

> »In current business, the validity of contracts is guaranteed by signatures. A signed contract serves as legal evidence of an agreement which the holder can present in court if necessary. The use of signatures, however, requires the transmission and storage of written contracts. In order to have a purely digital replacement for this paper instrument, each user must be able to produce a message whose authenticity can be checked by anyone, but which could not have been produced by anyone else, even the recipient.«

Auch Rivest, Shamir und Adleman (1978, 120) verweisen auf die Digitalisierung von Briefen als Anwendungsgebiet ihres Verschlüsselungsverfahrens:

> »The era of »electronic mail« may soon be upon us; we must ensure that two important properties of the current »paper mail« system are preserved: (a)

29 In der Praxis ist *n* meist 1024 Bit lang, wobei bereits 2048 Bit als Länge empfohlen wird (vgl. Paar/Pelzl 2016, 203).

30 Dieses Verfahren wird innerhalb der Kryptographie als *Textbook-RSA* bezeichnet, da es die Funktionsweise von RSA-Verschlüsselung schematisch verständlich macht, aber in der Praxis unsicher ist, da es deterministisch ist (vgl. Katz/Lindell 2008, 356). Mehrfaches Verschlüsseln eines gegebenen Plaintexts führt mit dieser Methode immer zu exakt demselben Ciphertext, was bedeutet, dass Angreifer_innen Informationen über die Kommunikationsinhalte ableiten können, die eigentlich geheim zu halten wären. Weiterführend zu sicheren Anwendungen von RSA siehe Katz/Lindell (ebd., 337–340).

> messages are private, and (b) messages can be signed. We demonstrate in this paper how to build these capabilities into an electronic mail system.«

Konkret geht es also sowohl Diffie und Hellman als auch Rivest, Shamir und Adleman darum, handschriftliche Unterschriften auf Papierdokumenten mittels asymmetrischer Kryptographie zu remediatisieren. Diffie und Hellman (1976, 649, Herv. i.O.) spezifizieren:

> »In order to develop a system capable of replacing the current written contract with some purely electronic form of communication, we must discover a digital phenomenon with the same properties as a written signature. It must be easy for anyone to recognize the signature as authentic, but impossible for anyone other than the legitimate signer to produce it. We will call any such technique *one-way authentication*.«

Rivest, Shamir und Adleman (1978, 121, Herv. i.O.) erweitern diese Forderungen mit Blick auf die medienspezifische Unmöglichkeit »to detect electronic ›cutting and pasting‹« innerhalb digitaler Datenverarbeitung: »An electronic signature must be *message*-dependent, as well as *signer*-dependent.« Zusammengefasst belaufen sich die Eigenschaften, über die digitale Unterschriften verfügen sollten, um handschriftliche Unterschriften auf Papierdokumenten zu ersetzen, auf 1) Authentizität der Signatur, 2) Fälschungssicherheit der Signatur, 3) Dokumentenbindung der Signatur, 4) Unveränderlichkeit des Dokuments nach der Unterschrift, und 5) Nicht-Zurückweisbarkeit der Signatur (vgl. Schneier 2015, 36). Eine digitale Signatur mittels *Textbook-RSA* würde folgendermaßen funktionieren: Person A verschlüsselt ein Dokument mit ihrem privaten Schlüssel und sendet es an Person B. Person B entschlüsselt das Dokument mit dem öffentlichen Schlüssel von Person A, und kann so die Unterschrift verifizieren (vgl. ebd., 37). Die Entschlüsselung des Dokuments verifiziert dabei die Authentizität der Signatur (1): Käme die Unterschrift beispielsweise von Person C, könnte die Entschlüsselung nicht mit dem öffentlichen Schlüssel von Person A durchgeführt werden. Die Fälschungssicherheit (2) der Signatur ist dadurch gegeben, dass sie mit dem privaten Schlüssel erstellt wird, auf den (in diesem Modell) ausschließlich Person A zugreifen kann. Da die Signatur sich mathematisch auf das signierte Dokument bezieht, ist sie dokumentenabhängig (3), und verhindert gleichsam die nachträgliche Veränderung des Dokuments (4), da eine solche die Signatur ungültig machen würde. Schlussendlich ist die Signatur nicht zurückweisbar, da sie unabhängig von der weiteren Mitarbeit der unterschreibenden Person

verifiziert werden kann (vgl. ebd., 37–38). Je nach Größe des unterschriebenen Dokuments ist diese Methode jedoch sehr zeit- und ressourcenaufwändig. Eine mögliche Lösung für dieses Problem besteht darin, nicht das Dokument selbst zu signieren, sondern mit einer Hashfunktion eine Prüfsumme des Dokuments zu erstellen, und diese zu signieren (vgl. ebd., 38–39). Dies hat ebenfalls den Vorteil, dass das Dokument selbst nicht verschlüsselt werden muss, und offen, aber unterschrieben versendet werden kann; oder aber, dass ein Dokument geheim gehalten werden kann, aber mittels der Signatur, die beispielsweise in eine Online-Datenbank hochgeladen wurde, und dadurch einen Zeitstempel erhalten hat, ein zeitkritischer Nachweis über die Autor_innenschaft eines Dokuments erbracht werden kann (vgl. ebd., 39).

Asymmetrische Kryptographie umfasst damit vier sogenannte *Sicherheitsdienste*:[31] Nichtzurückweisbarkeit, Schlüsselaustausch über unsichere Kanäle, Authentisierung/Identifikation und Verschlüsselung (vgl. Paar/Pelzl 2016, 178). Die Neuheiten gegenüber symmetrischer Kryptographie sind der Schlüsselaustausch über unsichere Kanäle, sowie die Möglichkeit *öffentlich*[32] überprüfbarer Signaturen. Darüber hinaus wird mit asymmetrischer Kryptographie, beispielsweise im Fall einer verschlüsselten E-Mail, eine versendete Nachricht mathematisch an den_die Empfänger_in gebunden, und, falls sie signiert wurde, ebenfalls an den_die Sender_in. Es können also sowohl die kommunizierenden Parteien als auch das jeweilige Dokument authentifiziert werden. So wird die Bezugnahme von Plaintext, Ciphertext, Empfänger_in und ggf. Sender_in aufeinander verhärtet.

---

31 Als *Sicherheitsdienste* werden »Schutzziele, die mit einem Sicherheitsmechanismus erreicht werden können« (Paar/Pelzl 2016, 297) bezeichnet.

32 Es existieren auch Signaturverfahren mit symmetrischer Kryptographie. Diese werden als *message-authentication schemes* bezeichnet. Der Unterschied von *message-authentication schemes* und asymmetrisch erzeugten Signaturen liegt in den Verifizierungsmöglichkeiten der jeweiligen Unterschriften (vgl. Goldreich 2009, 498). Durch die Trennung des öffentlichen und privaten Teils des Schlüssels bei asymmetrischer Kryptographie lassen sich Signaturen öffentlich verifizieren, da nur ein Teil des verwendeten Schlüssels für diesen Vorgang benötigt wird, wohingegen eine öffentliche Verifizierung einer symmetrisch erzeugten Signatur die Fälschungssicherheit und Personenbindung derselben aufheben würde, da der komplette Schlüssel dann bekannt ist.

2.5 Kryptographische Modellbildung

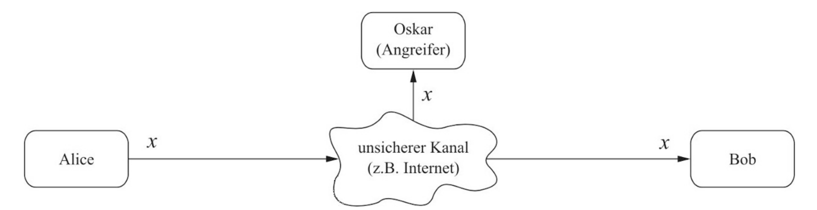
Anhand der bisher geschilderten Funktionsweisen kryptographischer Verfahren sowie der zwei formativen Schlüsselprobleme der Kryptographie ist ein Überblick über einige der wichtigsten Gegenstände sowie Theorieimpulse des Feldes entstanden. Dieser stellt die Grundlage für die weitere Analyse kryptographischer Modellbildung dar, im Zuge derer der Kanal, zwei berüchtigte Figuren und schlussendlich der innerfachlich zugrunde liegende Sicherheitsbegriff diskutiert werden wird. Zusammenfassend lässt sich als Hauptaufgabe der Kryptographie nach den bisherigen Ausführungen die Geheimhaltung einer Nachricht auf ihrem Weg von Sender_in zu Empfänger_in beschreiben. Der durch Verschlüsselung hergestellte Ciphertext ist die Remediatisierung eines Plaintexts, insofern der Vorgang der Verschlüsselung sich als prozessual auffassen lässt. Der Ciphertext wird nun wiederum durch Bot_innen, Telegraphie, das Internet etc. von Sender_in zu Empfänger_in übertragen. Diese jeweiligen Vorgänge, so lässt sich mit Kerckhoffs festhalten, müssen restlos reversibel sein, sodass am Ende der Kommunikationskette erneut die eingangs geschriebene Nachricht, der Plaintext steht. Auch asymmetrische Kryptographie folgt dem Prinzip einer restlosen Reversibilität, und bindet darüber hinaus (Sender_in und) Empfänger_in an die verschlüsselte (und signierte) Nachricht. So werden mit mathematischen Mitteln die Möglichkeiten der Verbreitung einer verschlüsselten Nachricht über den intendierten Weg hinaus beschränkt, und die Anwendungsbereiche von Kryptographie um Nichtzurückweisbarkeit und öffentliche Authentisierung erweitert, sowie eine mathematische Lösung für das Problem des Schlüsselaustauschs über den bisher mehrfach genannten *unsicheren Kanal* bereitgestellt, der im Folgenden genauer betrachtet wird.

2.5.1 Der *unsichere Kanal*

Ein repetitives Muster, das sich durch die Geschichte der Kryptographie zieht, wurde bisher noch nicht besprochen: Sowohl symmetrische als auch asymmetrische Kryptographie geht von einem Szenario aus, das gewissermaßen als Grundstruktur der Kryptographie beschrieben werden kann, in dem zwei räumlich voneinander getrennte Parteien miteinander kommunizieren wollen. Diese Kommunikation erfolgt über einen sogenannten *unsicheren Kanal*, der einer dritten Partei die Möglichkeit bietet, die Kommunikation abzufangen, zu belauschen, zu verändern, oder sich als eine der kommunizierenden

Parteien auszugeben. Paar und Pelzl (2016, 5) stellen diese Struktur schematisch dar:

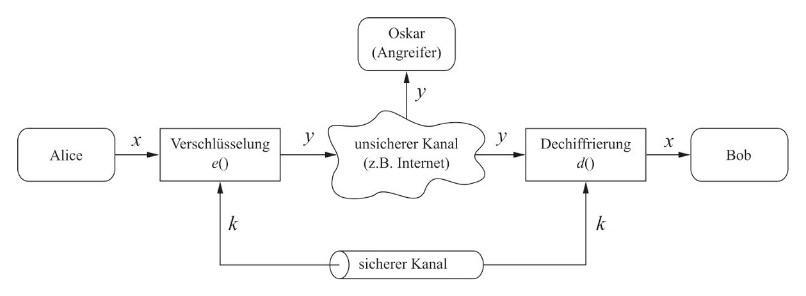
»Kommunikation über einen unsicheren Kanal mit lauschendem Gegenspieler«



Quelle: Paar/Pelzl 2016, 5

Bemerkenswert ist an dieser Stelle, dass nicht der Kanal, sondern der Weg der Nachricht »X« in der Grafik durch Pfeile visualisiert wird, wohingegen der unsichere Kanal als ein Zwischenraum dargestellt wird, in den die mit »X« bezeichnete unverschlüsselte Nachricht hineingegeben wird, und der die kommunizierenden Parteien »Alice« und »Bob« voneinander trennt. Eine solche Anordnung entspricht einer Sichtweise von Medien, die Sybille Krämer (2008, 16) als kennzeichnend für das sogenannte *technische Übertragungsmodell* von Kommunikation ausmacht: Medien sind zwischen Sender_in und Empfänger_in platziert, und gleichsam das, was »es überhaupt erst möglich macht, dass der Sender etwas ›aufgeben‹ kann, was dann beim Empfänger auch ankommt. Das Medium […] schafft eine Verbindung trotz und in der Entfernung.« Inwiefern ist dieser Kanal aber unsicher? Dies lässt sich anhand der Antwort der Kryptographie auf das durch die Grafik prägnant visualisierte Problem der als »Oskar« bezeichneten, eingreifenden dritten Partei beantworten. »Oskar« macht sich den unsicheren Kanal zunutze, um die versendete Nachricht abzuhören oder abzufangen – um dies zu verhindern, muss die Nachricht verschlüsselt werden. Dadurch schaffen die kommunizierenden Parteien, Paar und Pelzl (2016, 6) folgend, einen eigenen, *sicheren Kanal*, der an dem_der Angreifer_in vorbei führt:

»Verschlüsselung mit symmetrischer Kryptographie«



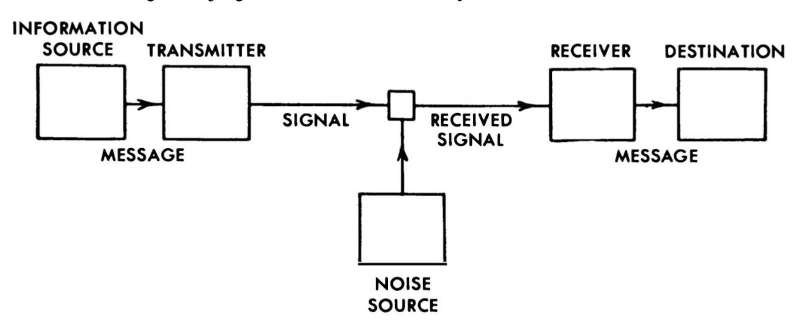
Quelle: Paar/Pelzl 2016, 6

Verschlüsselung macht dieser Darstellung zufolge also einen Kanal sicher. Bevor näher auf den Begriff »un/sicher« eingegangen wird, lohnt es, die Aufmerksamkeit zunächst noch einmal auf den Kanal zu richten. Als Beispiel für einen unsicheren Kanal wird in beiden Grafiken »z.B. Internet« angegeben. »Der leicht abstrakte Begriff ›Kanal‹«, schreiben Paar und Pelzl (ebd., 4) dazu, »bezeichnet lediglich die Kommunikationsstrecke, z.B. das Internet, eine Luftstrecke im Fall von WLAN oder Mobilfunk oder jedes andere Medium, über das sich digitale Daten übertragen lassen.« Die durch das Wort »lediglich« erzeugte Beiläufigkeit, und die scheinbare Beliebigkeit des Mediums lassen vermuten, dass Medien hier keine besondere Rolle zukäme, doch das Gegenteil ist der Fall. An dieser Stelle lässt sich ausführlicher mit Sybille Krämer (2008) anschließen, die sich in ihrem Buch *Medium, Bote, Übertragung. Kleine Metaphysik der Medialität* ausgehend von den Begriffen Kommunikation und Botengang der Übertragung als Medialitätsprinzip widmet. Krämer (ebd., 13) versucht zu Beginn ihrer Untersuchung, der Unschärfe des Begriffs »Kommunikation« beizukommen, indem sie anmerkt, dass der Ausdruck im aktuellen Diskurs ein »begriffliches Doppelleben« führe, das aus »zwei profilierten, jedoch gegenläufig zueinander stehenden Zusammenhängen, die wir hier das ›technische Übertragungsmodell‹ und das ›personale Verständigungsmodell‹ der Kommunikation nennen wollen«, bestehe. Als paradigmatisch für letzteres macht Krämer die Kommunikationstheorie Jürgen Habermas' aus, während für das technische Übertragungsmodell die Informationstheorie Claude Shannons und Warren Weavers grundlegend sei (vgl. ebd.). Das Ausgangsproblem des technischen Übertragungsmodells, so beschreibt es Krämer (ebd.), bestehe in der

> »räumlich/zeitlichen Entfernung zwischen Sender und Empfänger. Beide gelten als Instanzen, die menschlicher oder sächlicher Natur sein können und die Anfangs- und Endpunkte einer *linearen* Kette bilden, in der es unverzichtbare Zwischenglieder gibt, sei es in Gestalt des Mediums (Kanal), sei es in Form einer von außen kommenden ›Störgröße‹.«

In dieser Beschreibung findet sich ebenfalls das *Medium als Kanal*, wie es bereits bei Paar und Pelzl eingeführt wurde. Krämer (ebd., 14) schreibt weiter: »Die technische Verbindung ist dann erfolgreich, wenn es gelingt, in dem Übertragungsgeschehen vom Sender zum Empfänger den ›störenden Dritten‹ fernzuhalten.« Wer oder was der *störende Dritte* ist, ist abhängig davon, worauf der Blick fällt – für die Kryptographie ist es eine dritte Partei, die die Kommunikation zweier anderer abfangen möchte, für die mathematische Kommunikationstheorie von Claude Shannon (1964, 65) ein Nebenprodukt des Kanals, »noise«, Störgeräusche, die die Nachricht in der Übertragung verfremden können:

»Schematic diagram of a general communication system.«



Quelle: Shannon 1964, 34

Die strukturelle Gemeinsamkeit des *störenden Dritten* als Gefahr, aber auch der Anordnung im Allgemeinen lässt sich ebenfalls anhand der von Shannon entworfenen schematischen Darstellung des mathematischen Modells von Kommunikation erkennen. Über den Kanal, der als einziges Element der Grafik nicht mit einer Beschriftung ausgezeichnet ist, schreibt Shannon (ebd., 34, Herv. MS): »The channel is *merely* the medium used to transmit the

signal from transmitter to receiver. It may be a pair of wires, a coaxial cable, a band of radio frequencies, a beam of light etc.« Damit lässt sich Paars und Pelzls Beschreibung der Funktionsweise von Kryptographie als explizit an dem Shannonschen Modell orientiert erkennen.[33] Mit seiner Erläuterung des *transmitters*, »which operates on the message in some way to produce a signal suitable for transmission over the channel«, formuliert Shannon (ebd., 33) explizit aus, was bei Kerckhoffs bereits latent in der Forderung, Ciphertexte sollen telegraphisch[34] übertragbar sein, vorhanden ist: dass mit der Übermittlung einer (verschlüsselten) Nachricht ein Mediatisierungsvorgang verbunden ist. Anhand des Kerckhoffs'schen Prinzips und der damit einhergehenden Forderung nach Remediatisierbarkeit von Ciphertexten konnte in Kapitel 2.4.2 bereits gezeigt werden, dass die Telegraphie als Übertragungsmedium durch ihre Materialität und Medialität einen regulierenden Einfluss auf die Medialität, das heißt, auf die Übersetzungsleistung von Verschlüsselung nimmt. Shannon nimmt jedoch eine explizite Trennung zwischen dem Eingang einer Nachricht/Information in ein System an der Stelle des Transmitters, dem die Übersetzungsleistung zufällt, und deren augenscheinlich bloßer Übertragung über einen Kanal vor. Die Gleichsetzung von Medium und Kanal im Zusammenhang mit dieser Trennung erzeugt dabei zwei gegenständliche Medien, von denen eines ausschließlich übersetzt und eines ausschließlich überträgt. Diese Aufteilung verengt den Raum für die Betrachtung der *Medialität des Kanals*, und schließt Fragen nach dem, was als generatives Moment von Medien beschrieben werden kann, an dieser Stelle aus, die jedoch für eine medienwissenschaftliche Betrachtung von Kryptographie von Interesse wären. Anschließend an die bisherige Darstellung von Sybille Krämers medienphilosophischen Überlegungen soll hier daher erneut an die von ihr als zentral für die Medientheorie bestimmte Frage, ob Medien Sinn vermitteln oder erzeugen, angeknüpft werden. Mit Krämer lässt sich anhand des postalischen Prinzips von Medien, das in diesem Fall durch das technische Übertragungsmodell vorliegt, Medialität im Spannungsfeld von *Übertragung*

33 Warren Weaver (1964, 25) bemerkt in seinen Ergänzungen zu Shannons Theorie, dass die geringe Spezifizität des Modells dessen Stärke ausmache, da es auf alle Kommunikationssituationen übertragbar sei. »It is an evidence of this generality«, schreibt er weiter, »that the theory contributes importantly to, and in fact is really the basic theory of cryptography which is, of course, a form of coding.« (Ebd.)

34 Die Beliebigkeit des Mediums schränken auch Paar und Pelzl teilweise mit dem Hinweis auf digitale Datenübertragung ein.

und *Inkorporation* begreifen. Übertragung schließt hier an die Übertragung eines Mediums als Form in ein anderes Medium an, oder mit Bolters und Grusins Term: an die Remediatisierung. Diese Übertragung bestimmt Krämer (2003, 84) zugleich als eine schöpferische Geste, die nicht aus dem Nichts schafft, sondern durch die in der Übertragung geschehende Herstellung neuer Zusammenhänge, ähnlich wie dies bei der Bildung von Metaphern der Fall sei. Als Inkorporation definiert Krämer die Aktualisierung eines Musters, Schemas, einer Struktur, in der diese gleichsam eine Veränderung erfahre, die also über eine bloße »Fleischwerdung« (ebd.) hinausgehe, und den Raum der Betrachtung für die Performativität der Medialität öffnet. Wenn also »Medien im Akt der Übertragung dasjenige, was sie übertragen, zugleich mitbedingen und prägen«, kann »›Übertragung‹ als ›Konstitution‹« verstanden werden (ebd., 84–85). Shannons Trennung von Übersetzungsleistung und Medium, die Aufteilung von Medium und Mediatisierungsvorgang, sowie die Annahme, es gebe Einzelmedien, die sich mit Krämer (ebd., 85) als das »Resultat einer Abstraktion« begreifen lässt, ist eine wiederkehrende Figur technisch-mathematischer Diskurse, die nicht an der Reflexion von Medialität interessiert sind, sondern sich auf die technischen Apparate konzentrieren, die mit Krämer als Teil dessen, was Medien sind, verstanden werden können, in denen sich die Eigenschaften von Medien jedoch nicht erschöpfend zeigen. Diese Trennung ist historisch gewachsen, und erfüllt mehrere Funktionen: Die Verbindung und Interoperabilität zwischen verschiedenen Hard- und Softwarebestandteilen, die Möglichkeit, einzelne Elemente auszutauschen, was sowohl im Falle einer Störung als auch einer Aktualisierung einzelner Komponenten von Vorteil ist, sowie eine Vereinfachung der Fehlersuche, die gleichzeitig für die Ausfallsicherheit eines Systems eine große Rolle spielt. Infolgedessen erscheint der Kanal als neutrales Übertragungsmedium und die Herstellung von Sicherheit wird ebenfalls modularisiert: Sicherheit in der Informationstechnik und der Kodierungstheorie ist bezogen auf den Kanal und bedeutet Sicherheit einer Information vor *noise*. Darauf aufbauend befasst sich die Herstellung von Sicherheit in der Kryptographie damit, dass eine Nachricht auf dem Transportweg vor böswilligen Akteur_innen geschützt ist. Dies ist die Grundlage, auf der die innerfachlichen Diskurse von Kryptographie und IT-Sicherheit basieren.

2.5.2 Alice und Bob

> »Alice and Bob have a storied history. They send each other secrets, they get locked in jail, they get married, they get divorced, they're trying to date each other. I mean, anything two people might want to do securely, Alice and Bob have done it, somewhere in the cryptographic literature.« (Bruce Schneier [RSA Conference 2010, TC 1:04-1:17])

Die Bezeichnungen »Alice« und »Bob« für die beiden kommunizierenden Parteien in den Grafiken von Paar und Pelzl tauchen an dieser Stelle zum ersten Mal in der vorliegenden Untersuchung auf. Dies ist jedoch nicht repräsentativ für ihre Verwendung innerhalb der Fachliteratur der Kryptologie und IT-Sicherheit, in der Alice und Bob nahezu omnipräsent sind. Auch innerhalb popkultureller Kontexte erfreuen sich die beiden Figuren großer Beliebtheit, sind sie doch Teil dessen, was als »geek lore« (DuPont/Cattapan 2017, 1) bezeichnet werden kann: Alice und Bob haben einen eigenen Eintrag im *Jargon File* (vgl. The Jargon File o.J.a), tauchen hin und wieder im Webcomic *xkcd* auf (vgl. Munroe 2014; 2006), und es gibt eine Menge (unautorisiertes) Merchandise von ihnen zu kaufen. »More than just the world's most famous cryptographic couple«, schreiben Quinn DuPont und Alana Cattapan (2017, 1), »Alice and Bob have become an archetype of digital exchange, and a lens through which to view broader digital culture.« Im Folgenden soll der Blick nicht nur *durch*, sondern vor allem *auf* die Linse gerichtet werden: Wer und was sind Alice und Bob? Welche Rolle spielen sie für die Kryptographie?

Ein Großteil kryptologischer Fachliteratur behandelt, wie bereits herausgestellt, einen dem technisch-postalischen Übertragungsmodell folgenden Kommunikationsvorgang zweier Entitäten, seien es Personen oder Maschinen. Diese wurden gemeinhin als *A* und *B* unterschieden. Mit Ronald Rivests, Adi Shamirs und Leonard Adlemans bereits diskutiertem Paper *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* bekamen A und B die Namen, die sie bis heute behalten haben: »For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem« (Rivest et al. 1978, 121). Trotz dieser eher nüchtern-beiläufigen Einführung, aber vermutlich aufgrund der Praktikabilität der Namen, mit denen sich mathematische Beweisführungen, die zum größten Teil ausschließlich aus (mit Buchstaben bezeichneten) Variablen bestehen, übersichtlicher gestalten lassen, gewannen die Namen Alice und Bob innerhalb der wissenschaftlichen

Community an Popularität.[35] Mit den Namen zieht auch zum ersten Mal explizit die Geschlechterdifferenz in die kryptographische Modellbildung ein,[36] und macht Geschlecht über die Differenz adressierbar: Anhand von DuPonts und Cattapans (2017, 4) Bemerkung, dass A und B, bevor sie als Alice und Bob benannt wurden, »largely featureless« gewesen seien, was sie als »presumptively male, symbolic, and abstract« definieren, wird Androzentrismus als stille Norm sichtbar. Dies wird durch Ronald Rivests Aussage bestätigt: Die Geschlechter*differenz* sei mit der Absicht eingezogen worden, die kommunizierenden Parteien auch dann noch einfach unterscheiden zu können, wenn sie mit Personalpronomen bezeichnet werden – statt der zwei unmarkiert-männlichen Kommunizierenden A und B gibt es nun Alice, »she« und Bob, »he« (vgl. ebd., 7). DuPont und Cattapan (ebd., 9) verweisen darauf, dass auch Alice und Bob dennoch für einige Jahre, abgesehen von der Geschlechterdifferenz, zunächst ebenfalls als »featureless symbols – little more than named abstractions« verwendet worden seien. Dies sollte sich drei Jahre nach ihrem ersten Auftritt im Feld mit Manuel Blums Paper *Coin Flipping By Telephone. A Protocol For Solving Impossible Problems* ändern, das folgendermaßen beginnt:

> »Alice and Bob want to flip a coin by telephone. (They have just divorced, live in different cities, want to decide who gets the car.) Bob would not like to tell Alice HEADS and hear Alice (at the other end of the line) say »Here goes… I'm flipping the coin …. You lost!« (Blum 1983, 23)

DuPont und Cattapan (2017, 9) resümieren: »Blum's report is the first in what would become a tradition: literature that invents their situational context and backstory. […] From this point on, Alice and Bob have a history and, soon, will start to acquire personalities, and eventually friends.« Von diesem Moment an sind Alice und Bob manchmal verheiratet, manchmal geschieden, und manchmal einfach nur zwei Personen, die nur aufgrund einer gegebenen Situation miteinander in Kontakt treten: In der Phantasie der Forscher_innen, die ihre Geschichten schreiben, entwickeln sie eine Art Eigenleben. Einen Überblick

35 Die Bedeutung und Bekanntheit der ersten nach dem Prinzip der asymmetrischen Kryptographie funktionierenden Verschlüsselungsmethode, die Rivest, Shamir und Adleman entwarfen, wird sicher ihren Teil zur Popularität von Alice und Bob beigetragen haben.

36 In den Computern, die für die kryptographischen Berechnungen und die Übermittlung verschlüsselter Nachrichten verwendet werden, ist die Geschlechterdifferenz bereits mit dem Turing-Test eingezogen (vgl. Bergermann 2018, 339–340; Draude 2017, 190–194).

über die vielfältigen Situationen, in die Alice und Bob hineingeschrieben wurden, liefert nur ein Jahr nach Blum die anekdotisch gehaltene *After Dinner-Speech* des Kodierungstheoretikers John Gordon. Und tatsächlich haben Alice und Bob ein bewegtes Leben, das sich auch nicht mehr nur auf die Kryptologie beschränkt, sondern sich sukzessive auf weitere Disziplinen ausweitet: »Over the years Alice and Bob have tried to defraud insurance companies, they've played poker for high stakes by mail, and they've exchanged secret messages over tapped telephones« (Gordon 2007, 344). Gordon (ebd.) merkt scherzhaft an, sein Vortrag »may be the first time a definitive biography of Alice and Bob has been given« – tatsächlich liefert er allerdings nicht nur eine Biographie, sondern gleichsam einen Überblick über die verschiedenen Funktionalitäten, die Kryptographie in sich vereint. Ein fiktives Szenario sticht dabei besonders hervor, da es mit Katz und Lindell (2008, 3) exemplarisch für das erweiterte Anwendungsgebiet moderner Kryptographie steht, zu dem »problems of message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, digital cash and more« zählen:

> »So you see Alice has a whole bunch of problems to face. Oh yes, and there is one more thing I forgot to say – Alice doesn't trust Bob. We don't know why she doesn't trust him, but at some time in the past there has been an incident. Now most people in Alice's position would give up. Not Alice. She has courage which can only be described as awesome. Against all odds, over a noisy telephone line, tapped by the tax authorities and the secret police, Alice will happily attempt, with someone she doesn't trust, whom she cannot hear clearly, and who is probably someone else, to fiddle her tax returns and to organize a coup d'etat, while at the same time minimizing the cost of the phone call.« (Gordon 2007, 345)

Da der Kodierungstheoretiker Gordon seinen Vortrag mit dem Satz »A coding theorist is someone who doesn't think Alice is crazy« (ebd.) schließt, folgern DuPont und Cattapan, dass auch Gordon Alice und Bob letztlich nur »for their typical purpose: as means to an explanatory end« (DuPont/Cattapan 2017, 10) gebrauche. Die Geschichten von und mit Alice und Bob lediglich als ein (pädagogisches) Mittel zum Zweck zu verstehen, wäre jedoch zu kurz gegriffen, denn, wie Haraway (1997, 125) bemerkt: »Stories are not ›merely‹ anything.« DuPont und Cattapan benennen Alice und Bob zwar ebenfalls als »tropes of cryptology research«, dennoch suggeriert die Kritik, die sie an Gordon üben, ein flacheres Verständnis von *tropes*, als an dieser Stelle produktiv wäre. Die

Geschichten von Alice und Bob, mit denen Paper wie auch Lehrbücher beginnen, stellen einen Bezug her zwischen Kryptographie und dem (eigenen) Alltag. Damit qualifizieren sich Alice und Bob für pädagogische Zwecke – doch sie dienen dort nicht nur als Mittel zum Zweck, sondern arbeiten an den Modellen mit, indem mit ihren Geschichten eine konkrete Situation mit den dazugehörigen Regeln, Einschränkungen, und Zielen erläutert und verkörpert werden kann. Ulrike Bergermann (2016, 280) schreibt in ihrer Untersuchung der Gründungsdiskurse von Kybernetik und Medienwissenschaft, die Rolle von Modellen liege in »der Verminderung der Komplexität von Theorie«. Modelle

> »[...] vermitteln zwischen Spekulationen und Experimenten, sie verzahnen Natur mit Theorie, und ihr Bau findet in einem Zwischenraum zwischen Phänomenen und Theoriebildung statt, in einer Darstellung, die dem menschlichen Denken und Wahrnehmen angepasst ist, auch wenn ein Fachvokabular noch gar nicht existiert.« (Ebd.)

Modelle schaffen ein Verständnis für einen konkreten Fall, aber auch die Gesetzmäßigkeiten, in die er eingebettet ist, ohne dass, wie Bergermann herausstellt, bereits ein Fachvokabular vorhanden sein muss. Dies ist möglich, da die erzählte modellhafte Geschichte die Gesetzmäßigkeiten einer problematisierten Situation so verkörpert, dass diese in den jeweiligen kryptologischen Schriften aus ihr abgeleitet werden können.[37] Im Fall der Kryptographie, ließe sich hier einwenden, gehe es jedoch weniger darum, »Natur« mit »Theorie« zu verzahnen, schließlich könne nicht behauptet werden, dass diese – wie beispielsweise Physik oder Biologie – Bezug auf ein in der Welt vorhandenes Material nehme, um dieses mit wissenschaftlicher Theoriebildung zu einem Gegenstand zu verschmelzen, kurz: es könne nicht behauptet werden,

37 Bei Blum ergeben sich also aus der eingangs geschilderten Situation, dass Alice und Bob sich nach einer Scheidung telefonisch per Münzwurf darauf einigen wollen, wer das Auto bekommt, bereits folgende Gesetzmäßigkeiten: 1.) Alice und Bob vertrauen sich nicht (mehr), weswegen das entwickelte Verfahren so aufgebaut sein muss, dass keine Partei die andere hintergehen kann; 2.) sie leben in verschiedenen Städten und können (oder wollen) sich daher nicht treffen, was die Notwendigkeit der Entwicklung eines komplexen Verfahrens bedingt – ansonsten hätten sie einfach bei einem gemeinsamen Treffen in leiblicher Ko-Präsenz eine Münze werfen können – wodurch auch das Erkenntnisinteresse des Aufsatzes plausibilisiert wird. Bemerkenswert ist an dieser Stelle auch, in welcher Weise klischeehaft-heteronormative Erzählstrategien an den Gesetzmäßigkeiten und ihrer Plausibilisierung mitarbeiten.

dass Mathematik ebenfalls situiertes Wissen produziere.[38] Mit Donna Haraway lässt sich dieser Einwand entkräften: Anhand eines von Helen Watson-Verran und David Turnbull durchgeführten Vergleichs europäischer Praktiken formaler Logik mit denen der Yolngu, eines indigenen australischen Volksstammes, bemerkt Haraway (2018, 140), dass die Praktiken zwar ähnlich seien, der konstituierende Prozess der Kategorienbildung sich jedoch signifikant unterscheide. Daraus folgt für Haraway (ebd.):

> »Full of tropes, mathematics is specific material-semiotic practice at every level of its being, without ceasing to be of fundamental interest in terms of processes of cognition and products of formal knowledge. Mathematical knowledge is situated knowledge.«

Was Haraway hier für die Mathematik konstatiert, gilt auch für die neuere Kryptographie, deren elementarer Kern aus Mathematik besteht. Auch die Kryptographie erzeugt situiertes, also materiell-semiotisches Wissen, das gebunden ist an Mathematik, Medialität und, nicht zuletzt, an Alice und Bob als *Trope*. »In Greek«, führt Haraway (1997, 125) aus, »*tropos* means a turning; and the verb *trepein* means to swerve, to not get directly somewhere. Words (not to mention sentences) trip us, make us swerve, turn us around; and we have no other options.« Es gibt folglich kein *eigentliches Sprechen*, keine Alternative »to going through the medium of thinking and communicating, no alternative to swerving, materially« (ebd.). *Tropism* ist für Haraway nicht nur mit Metaphern verbunden, sondern auch mit Modellen. Letztere sind, so schreibt sie, ob konzeptuelle oder physische, *uneigentliches Sprechen* »in the sense of instruments built to be engaged, inhabited, lived« (Haraway 2018, 135). Mit den Jahren sind verschiedene Figuren entstanden, die mit Alice und Bob die Modell-Geschichten bewohnen. Spätestens mit Bruce Schneiers (Lehr-)Buch *Applied Cryptography*, das 1994 zum ersten Mal erschien, wurden diese Figuren im Feld kanonisiert: In einer mit »Dramatis Personae« betitelten Tabelle listet Schneier (2015, 23) außer Alice und Bob noch Carol (»Participant in the three- and four-party protocols«), Dave (»Participant in the four-party protocols«), Eve (»Eavesdropper«), Mallory (»Malicious active attacker«), Trent (»Trusted arbitrator«), Walter (»Warden; he'll be guarding Alice and Bob in

38 Dies kann durchaus als das Erbe der im Europa des 19. Jahrhunderts herausgebildeten *formalistischen Mathematik* aufgefasst werden, innerhalb derer die Mathematik als ein in sich geschlossenes System ohne Bezug auf etwas, das ihr äußerlich sei, konzeptualisiert wurde (vgl. Heintz 1993, 16).

some protocols«), Peggy (»Prover«), und Victor (»Verifier«) auf. Mit »Dramatis Personae« werden in der Regel vor Beginn des Dramentexts die handelnden Personen eines Bühnenstücks und deren Rolle in demselben eingeführt – bei Schneier sind es die Protagonist_innen kryptographischer Protokolle, also festgelegter, sich wiederholender Abläufe. Die Wiederholung der Charaktere in Geschichten, die oftmals heterosexuelle Paarbeziehungen durch Heirat, Scheidung oder Dating von Alice und Bob thematisieren, arbeiten auf mehreren Ebenen: Sie bringen einerseits das Geschlecht der Figuren hervor, insofern Geschlechtsidentität wie Judith Butler (2002, 302, Herv. i.O.) formuliert, »durch eine *stilisierte Wiederholung von Akten* zustande kommt«, und entwerfen darüber hinaus eine heteronormative Ordnung. Weiterhin lassen sich durch die Wiederholung der Charaktere, die durch ihre Rollen sinnbildlich für spezifische kryptographisch relevante Aktionen stehen, die geschilderten Alltagssituationen nicht nur in ein Modell übersetzen, sondern werden die Alltagssituationen als kryptographische Systeme *formalisiert*, und gewinnen damit nicht nur einen deskriptiven, sondern auch einen präskriptiven Charakter. Alice und Bob sind damit in Haraways Sinne *Figuren*, sind *Tropen*, die nicht nur ins Denken bringen, sondern dieses Denken mitgestalten. Mit Alice und Bob sind die Geschichten, die Modelle, aber auch die mathematischen Beweisführungen und Ergebnisse der Kryptographie »tropic to the core and *therefore* part of knowledge practices« (Haraway 2018, 141, Herv. i.O.), die die mit ihnen eingeleiteten kryptographischen Verfahren an zeitgenössische gesellschaftliche Fragen und Begehren rückbinden.

Ent/Politisierungen

»In den computertechnischen Schriften«, formuliert Ulrike Bergermann (2018, 339) in *biodrag. Turing-Test, KI-Kino und Testosteron*, »kommen Kultur und Gesellschaft in der Regel nicht vor – nur in den Beispielen zu den Regeln schlendern sie wieder hinein; für die Wissenschaft erschienen sie ausgegliedert, in die Kultur, die Fiktionen, in Filme.« So entsteht der Eindruck von Selbstgenügsamkeit eines scheinbar in sich geschlossenen Systems, obwohl bereits in Alan Turings *Imitationsspiel* Gender »grundlegend in die Modellierung eingetragen« war, was jedoch, wie Bergermann (ebd., 340) ausführt, »durch die Folgemodellierer, die Computergeschichte schreiben, ostentativ ausgeblendet« worden war. Mit Alice und Bob schlendern, wie gezeigt wurde, Kultur und Gesellschaft, sowie »Lust, Liebe, Begehren« (ebd., 339) im Feld der Kryptographie allerdings nicht nur in den Beispielen zu den Regeln, sondern auch in die Expositionen der Probleme und in die Modellbildung hinein.

So halten mit diesen Geschichten, die mal absurde, mal verhältnismäßig realistische (Alltags-)Situationen schildern, im Vergleich zu ihrer ca. 4000 Jahre alten, überwiegend militärischen Geschichte eine Vielzahl an gesellschaftlichen Zusammenhängen und Begehren in das Feld der Kryptographie Einzug.

Dies drückt sich auch in den Visualisierungen von Alice und Bob aus, die nicht lange auf sich warten ließen. Wurden in Schneiers *Applied Cryptography* in einer direkt auf die tabellarische Übersicht der »Dramatis Personae« folgenden Grafik, die verschiedene kryptographische Protokolle veranschaulicht, Alice, Bob und Trent noch nicht als Personen, sondern als Häuser dargestellt (vgl. Schneier 2015, 24), so sollte sich dies in den darauf folgenden Jahren mit dem Zusammenwachsen von Kryptologie und Informatik im Bereich der IT-Sicherheit verändern, nicht zuletzt durch die Popularisierung von computergestützten Präsentationen und Clip-Art: »[F]aculty began to portray Alice and Bob in a classroom setting using clip art and other images that personified Alice and Bob (usually in white, heteronormative,[39] and gendered ways) […].« Als Gegenprogramm zu der scheinbar selbstverständlichen *Whiteness* von Alice und Bob in diesen Darstellungen schlug der indische Kryptograph Srini Parthasarathy (2012, 4) vor, Alice und Bob durch *Sita* und *Rama* zu ersetzen. Parthasarathy (ebd., 2) sieht zwei Vorteile in dieser Ersetzung: Zum einen, dass Sita und Ramas Anfangsbuchstaben mit den Anfangsbuchstaben von *sender* und *receiver* übereinstimmen. Zum anderen, dass eine Szene aus der Geschichte von Sita und Rama in der hinduistischen Mythologie, genauer im *Sundara Kanda*, dem fünften Buch des *Ramayana*, dem technisch-postalischen Übertragungsmodell, und damit der initialen Situation der Kryptographie bereits sehr ähnlich ist: Sita wurde von Ravana entführt und in einem Wald gefangen gehalten. Sie wird von Hanuman aufgesucht, einer hinduistischen Gottheit in Gestalt eines Affen, der von Rama geschickt wurde, was er durch einen Ring Ramas nachweisen kann. Sita gibt Hanuman eine Nachricht, die er an Rama übermitteln soll. Als Nachweis, dass die Nachricht wirklich von ihr ist, gibt Sita Hanuman ein Schmuckstück von ihr mit. Parthasarathy (ebd., 2–3) folgend entspräche Hanuman dem Medium oder Kanal, und Ravana, der die Nachricht abfangen möchte, dem *störenden Dritten*. Diese Geschichte kann, wie Parthasarathy

39 DuPont und Cattapan (2017, 11–12) führen dazu die Entwicklung von Eve (eavesdropper) von einer lauschenden Partei ohne spezifischem Interesse an, das sich mit der Zeit zum Bild von Eve als verlassener Frau wandelte, die die Kommunikation ihres Ex-Partners Bob mit dessen neuer Partnerin Alice belauscht.

ausführt, modellhaft sowohl für Verschlüsselung als auch für digitale Signaturen verwendet werden. Parthasarathys Vorschlag stieß jedoch, wie er anmerkt, nicht auf viel Zustimmung: »Some people […] seemed to have issues with using Hindu names, adding a religious and xenophobic flavour to the conversation« (ebd., 4), was sich als Zeichen sowohl der *Whiteness* von Alice und Bob als auch des innerfachlichen Diskurses der Kryptographie und der IT-Sicherheit sowie der rassistischen Exklusionsmechanismen akademischer Institutionen der westlichen Welt lesen lässt.

Die (Clip-Art-)Darstellungen von Alice und Bob sind darüber hinaus auch Bestandteil der Kritik des US-amerikanischen Kryptographen Phillip Rogaway an der Ausrichtung der Kryptographie als akademischer Disziplin. In seinem Vortrag mit dem Titel *The Moral Character of Cryptographic Work* ermahnt Rogaway seine eigene wissenschaftliche Community, nicht zu vergessen, dass Kryptographie in Machtverhältnisse eingebettet ist, und auch an diesen mitarbeitet. Dieser Umstand werde innerhalb des Fachs selbst nicht oft thematisiert, wie er zugespitzt formuliert:

> »Most academic cryptographers seem to think that our field is a fun, deep, and politically neutral game – a set of puzzles involving communicating parties and notional adversaries. This vision of who we are animates a field whose work is intellectually impressive and rapidly produced, but also quite inbred and divorced from real-world concerns.« (Rogaway 2015, 1)

Diese Art des Denkens wird von Rogaway (ebd., 16) heftig kritisiert: »Some might think that a community's focus is mostly determined by the technical character of the topic it aims to study. It is not. It is extra-scientific considerations that shape what gets treated where.« Einen Teil dieser außerhalb der Wissenschaft stehenden Überlegungen machen für Rogaway die zur Zeit des Vortrags erst zwei Jahre alten Enthüllungen des Whistleblowers Edward Snowden aus, die eine noch nicht da gewesene Form der Massenüberwachung von Bürger_innen der ganzen Welt durch Geheimdienste offenbarten. In seinem Vortrag macht Rogaway seinem Unmut darüber Luft, dass die akademische kryptographische Community nach den Snowden-Enthüllungen scheinbar keinen Handlungsbedarf sehe, und legt anhand eines Exkurses dar, dass es keine unpolitische Wissenschaft geben könne, lediglich eine (falsche) Leugnung der eigenen Verantwortung als Wissenschaftler_in. Das in der Einleitung seines Arguments aufgerufene Bild des Puzzles hat wissenschaftsgeschichtlich durchaus Tradition: Der Wissenschaftshistoriker

Thomas Kuhn, dessen Buch *The Structure of Scientific Revolutions*[40] sich mit der Rolle von wissenschaftlichen Paradigmen, Paradigmenwechseln und der Konzeptionalisierung von wissenschaftlichem Fortschritt befasst, geht ausführlich auf das Lösen von Puzzles als Teil der Herstellung von Wissen der sogenannten »normal science«[41] (dt.: *normale Wissenschaft*) ein. Eine der bemerkenswertesten Eigenschaften der Forschungsfragen *normaler Wissenschaft* sei laut Kuhn (1996, 35), »how little they aim to produce major novelties, conceptual or phenomenal.« Sie würden dennoch gestellt und bearbeitet, da sie dazu beitragen, das zu einem gegenwärtigen wissenschaftlichen Paradigma gehörende Wissen zu verfeinern und zu erweitern (vgl. ebd., 36). Was die beteiligten Wissenschaftler_innen motiviere, sich solchen Forschungsfragen zu widmen, deren Ergebnisse bereits zu antizipieren seien, erklärt sich für Kuhn durch die motivierende Wirkung des Puzzle-Lösens, und damit durch die höhere Bewertung des Weges als des Ergebnisses: »Bringing a normal research problem to a conclusion is achieving the anticipated in a new way, and it requires the solution of all sorts of complex instrumental, conceptual, and mathematical puzzles« (ebd.).[42] Ebendiese Puzzles stellen Kuhn zufolge eine eigene Kategorie wissenschaftlicher Probleme dar, für die Einfallsreichtum und Fähigkeit in der Bearbeitung eher im Vordergrund stünden als dass das Problem eine interessante oder wichtige Lösung habe

40 Kuhns Überlegungen zum Paradigma in der Wissenschaft waren grundlegend für Donna Haraways Diskussion der Metapher, wie sie in *Crystals, Fabrics, and Fields. Metaphors of Organicism in Twentieth-Century Developmental Biology* darlegt (vgl. Haraway 1976, 1–32). Aus diesen Überlegungen entstand sukzessive Haraways erweiterter Begriff der *Trope*.

41 Als *normale Wissenschaft* definiert Kuhn (1996, 10) »research firmly based upon one or more past scientific achievements, achievements that some particular scientific community acknowledges for a time as supplying the foundations for its further practice.« Moderne Kryptographie lässt sich damit im Sinne Kuhns als *normale Wissenschaft* klassifizieren.

42 Kuhn (1996, 36) zieht explizit Parallelen zwischen Puzzles als wissenschaftlicher Problemkategorie und Puzzles und Kreuzworträtseln (englisch: crossword *puzzles*) als Alltagsgegenständen, und geht darauf ein, dass das Lösen eines Puzzles einen Forschungsanreiz darstelle: »The man who succeeds proves himself an expert puzzle-solver, and the challenge of the puzzle is an important part of what usually drives him on.« Was an dieser Stelle spannend wäre, aber leider zu weit führen würde, wäre anhand des vom britischen Geheimdienst GCHQ herausgegebenen *GCHQ Puzzle Book* (vgl. MacAskill 2018) genauer über den Status wissenschaftlicher Puzzles als Spiele nachzudenken.

(vgl. ebd., 36–37) – das *wie* ist in diesem Fall also bedeutsamer als das *was*.[43] Der bisher dargelegte repetitive Charakter kryptographischer Forschung, der sich sowohl für *klassische*, und später für *moderne* Kryptographie im zugrunde liegenden technisch-postalischen Übertragungsmodell zeigt, hat größtenteils Forschungsfragen hervorgebracht, die sich mit Kuhn als ebendieser Kategorie von Puzzles zugehörig beschreiben lassen. Alice und Bob haben dabei, wie bereits dargelegt wurde, ihren illustrativen Charakter hinter sich gelassen, und sind mit Haraway als Trope zu verstehen: Die von ihnen ausgehend erzählten Geschichten, ihre Probleme, die es zu lösen gilt, bringen Forscher_innen ins Denken. Allerdings, und dies ist der Ansatzpunkt von Rogaways Kritik, in ein entpolitisiertes Denken, das durch die Darstellungskonventionen der Charaktere hervorgerufen werde:

> »There is a long tradition of cutesiness in our field. People spin fun and fanciful stories. Protocol participants are a caricatured Alice and Bob. Adversaries are little devils, complete with horns and a pitchfork. Some crypto talks are so packed with clip-art you can hardly find the content. I have never liked this, but, after the Snowden revelations, it started to vex me like never before.« (Rogaway 2015, 41)

Rogaway fordert eine Bereinigung der Kryptographie von ihrer lieb gewonnenen Trope, die sich nahezu memetisch durch Präsentationen, Paper und das Denken der Community zieht. Einerseits, da diese Figuren seiner Wahrnehmung nach überhandnehmen, und anstatt Sachverhalte verständlicher zu gestalten, einen »layer of obfuscation« erzeugten, »that must be peeled away to understand what has actually been done« (ebd., 41). Andererseits, da die Geschichten und Probleme der fiktiven Charaktere von den eigentlichen Gegenspielern ablenkten, was Konsequenzen für die Forschung habe:

> »Worse, the cartoon-heavy cryptography can reshape our internal vision of our role. The adversary as a $53-billion-a-year military-industrial-surveillance complex and the adversary as a red-devil-with-horns induce entirely different thought processes. If we see adversaries in one of these ways, we will actually see at a different set of problems to work on than if we see things in the other.« (Ebd., 41–42)

43 Kuhn (1996, 37–38) konstatiert, dass solche Puzzles eine motivierende Anziehungskraft auf »the proper sort of addict« (ebd., 38) – also auf Wissenschaftler_innen – ausüben würden, die in einer Vielzahl an Möglichkeiten begründet liegen könne, aufgrund derer eine Person sich dazu entschließen könne, zu forschen.

Diese Entpolitisierung, die Rogaway, wie er mehrfach betont, vor allem nach den Snowden-Enthüllungen untragbar erscheint, verstelle den Blick auf den titelgebenden *moral character* der eigenen Arbeit: Sie lenke von der Frage ab, welche Probleme aus Sicht der Geheimdienste, die er als die eigentlichen Gegenspieler identifiziert, von der Wissenschaft lieber *nicht* gelöst werden sollten (ebd., 42). Rogaway kritisiert darüber hinaus die monetäre Verstrickung der Universitäten mit Geheimdiensten, und macht sich daran, die innerfachlich diskursiv entpolitisierte Kryptographie wieder aktiv zu politisieren:

> »I have heard it said that if you think cryptography is your solution, you don't understand your problem. If this quip is true, then our field has gone seriously astray. But we can correct it. We need to make cryptography the solution to the problem: ›how do you make surveillance more expensive?‹« (Ebd., 46)

Ist das also das Ende von Alice und Bob? Rogaways Kritik war vermutlich weniger einflussreich, als er gehofft haben dürfte. Alice und Bob sind wohlauf, und ihr Einfluss auf das Feld scheinbar ungebrochen. Es dürfte sich darüber hinaus als unmöglich erweisen, sich einer Trope vorsätzlich gänzlich entledigen zu wollen, denn schließlich sind Tropen an der Herstellung von Wissen beteiligt und daher mit diesem verwoben. Sich der Frage zu widmen, wie Massenüberwachung teurer – und damit erschwert oder verhindert werden könne – ist erfreulicher Weise dennoch zum Problem zeitgenössischer Kryptographie geworden (vgl. exemplarisch Auerbach et al. 2018; Bellare et al. 2014; Degabriele et al. 2015). Umformuliert könnte Rogaways Frage lauten: Wie kann man vor Massenüberwachung sicher sein? Dies führt zum letzten Teil dieses Kapitels, in dem abschließend darauf eingegangen wird, wie innerhalb der Kryptographie definiert wird, was *Sicherheit* ist.

2.5.3 Sicherheit in der Kryptographie

In den bisherigen Ausführungen ist deutlich geworden, dass klassische, aber auch moderne Kryptographie sich hauptsächlich damit befasst, eine Nachricht, die über einen als *unsicher* definierten Kanal gesendet wird, auf dem Transportweg vor einem *störenden Dritten* zu schützen – gelingt dies, so wurde entsprechend Sicherheit geschaffen. Mit dem Übergang von klassischer zu moderner Kryptographie und der Herausbildung von Kryptologie als Wissenschaft wurde auch innerhalb der noch vergleichsweise jungen Disziplin Sicherheit definiert, allerdings stets basierend auf dem technisch-postalischen Übertragungsmodell. Diese Definitionen befassen sich entsprechend

mit der Frage, welche Anforderungen an kryptographische Mechanismen gestellt werden müssen, damit ein System als sicher gilt. Ein Alternative zum technisch-postalischen Übertragungsmodell wird dabei jedoch nicht gesucht, und dementsprechend auch nicht über die Eigenschaften (und daraus resultierenden Beschränkungen) des zugrunde liegenden Sicherheitsbegriffs nachgedacht. Im Folgenden soll daher anhand eines Teilbereichs der Kryptographie namens *Beweisbare Sicherheit* (eng.: provable security, vgl. Koblitz 2007, 976) dargelegt werden, wie Sicherheit innerhalb der Disziplin Kryptographie weitergehend definiert wird. In einem zweiten Schritt soll diese Definition in einem größeren Kontext situiert werden.

Rigorose Definitionen

Moderne Kryptographie zeichnet sich im Vergleich zu klassischer Kryptographie wie bereits mehrfach bemerkt vor allem dadurch aus, dass Kryptographie von einer Kunst zu einer Wissenschaft geworden ist. Dieser Übergang ist verbunden mit der Formulierung einer rigorosen, also strengen Methodologie, sowie der Explizierung ansonsten unausgesprochen bleibender Vorannahmen, um Fortschritt herstellen und beurteilen zu können, sowie eine generelle Vergleichbarkeit der erfundenen Verfahren zu gewährleisten. Eines der Hauptkriterien dafür ist, dem Kryptographen Oded Goldreich (2004, 21) folgend, ein »rigorous treatment«, oder Jonathan Katz und Yehuda Lindell (2008, 18) folgend, eine »rigorous and precise definition of security«. Was Goldreich 2004 in *Foundations of Cryptography* über die Methode und die Notwendigkeit einer festen Definition von Sicherheit darlegt, nämlich die Notwendigkeit, ein kryptographisches System auf »firm foundations« (Goldreich 2004, 21) und nicht auf Heuristiken oder Intuitionen aufzubauen, sowie seine Überlegungen zur Wichtigkeit unbewiesener Annahmen darüber, was in welcher Zeit mit Computern berechnet werden kann (vgl. ebd., 22), lässt sich als Kernelement dessen beschreiben, was Katz und Lindell vier Jahre später als die drei Prinzipien moderner Kryptographie ausmachen. Das erste Prinzip besagt, dass für das Lösen eines kryptographischen Problems die bereits genannte Formulierung einer »rigorous and precise definition of security« (Katz/Lindell 2008, 18) notwendig sei. Diese sei aus verschiedenen Gründen wichtig: Erstens, um sicherzustellen, dass für ein gegebenes Sicherheitsproblem eine adäquate kryptographische Lösung designt wird, und das Design nicht erst nach Fertigstellung auf die notwendigen Funktionen hin überprüft wird; zweitens, da eine solche Definition eine Vergleichbarkeit verschiedener kryptographischer Systeme im Hinblick auf ihre Sicherheitsdienste und Effizienz

ermöglicht, und so eine Auswahl für ein konkretes Problem getroffen werden kann; und drittens, um eine generelle Vergleichbarkeit hinsichtlich mehr Faktoren als Effizienz und Sicherheitsdienste verschiedener kryptographischer Systeme herstellen zu können (vgl. ebd., 19). Nicht zuletzt ist es auch eine rigorose Sicherheitsdefinition, die es erlaubt, einen *rigorosen Beweis* für die Sicherheit eines gegebenen Systems zu geben (vgl. ebd., 20), denn nur wenn die Ansprüche an ein System klar definiert worden sind, kann eine Aussage darüber getroffen werden, ob sie eingehalten wurden. Darüber hinaus wenden sich Katz und Lindell (ebd., 20) explizit gegen die Annahme, eine formale Definition von Sicherheit sei nicht notwendig, da intuitiv klar sei, was *sicher* bedeute – selbst ein und dieselbe Person könne kontextabhängig unterschiedliche Vorstellungen dazu haben. Nach einigen beispielhaften Annäherungen stellen Katz und Lindell (ebd., 22) basierend auf dem ersten Prinzip moderner Kryptographie eine grundsätzliche Sicherheitsdefinition für moderne Kryptographie auf: »A cryptographic scheme for a given task is secure if no adversary of a specified power can achieve a specified break.« Durch die exponierte Position des zu verhindernden Brechens eines kryptographischen Systems schließt diese Definition auch an die von Kerckhoffs formulierte Wichtigkeit der Kryptanalyse für die Evaluierung kryptographischer Methoden an (vgl. Kahn 1967, 234–235). Der_die Angreifer_in bleibt bei Katz und Lindell dabei an einer entscheidenden Stelle absichtlich unterdeterminiert: Die vorgelegte Definition trifft zwar Aussagen über die Fähigkeiten des_der Angreifer_in, aber keine Aussagen über die gewählte Methode des Angriffs. Dies bezeichnen sie als »arbitrary adversary principle« (Katz/Lindell 2008, 22).[44] Auch Goldreich (2004, 21) geht darauf ein, dass es nutzlos sei, die Strategie des_der Gegner_in vorauszuplanen, da diese_r sich per se nicht an die Spielregeln halte: »the adversary will try to take actions other than the ones the designer has envisioned.« Annahmen über die Ressourcen der angreifenden Partei seien hingegen gerechtfertigt und notwendig (vgl. ebd.).

Das zweite Prinzip moderner Kryptographie besagt, dass wenn die Sicherheit eines kryptographischen Verfahrens auf einer unbewiesenen Annahme

44 Die Unterdeterminiertheit der angreifenden Partei zeigt sich auch in den Figuren, die den Angreifer_innen zugewiesen werden: Schneiers (2015, 23) »Dramatis Personae« beinhalten *Eve* und *Mallory*, die sich lediglich dadurch unterschieden, dass *Eve* (»eavesdropper«) passiv lauscht, und *Mallory* (»malicious active attacker«) aktiv angreift – wie genau dies durchgeführt wird, wird nicht beschrieben. Paar und Pelzls (2016, 4) *Oskar* (vermutlich abgeleitet von »Opponent«) ist ebenfalls nicht näher bestimmt.

basiert, diese so präzise und reduziert wie möglich zu definieren sei (vgl. Katz/ Lindell 2008, 18). Katz und Lindell (ebd., 25) führen die schwere Lösbarkeit bestimmter mathematischer Probleme als Beispiel einer solchen unbewiesenen Annahme ein. Dieser Fall ist gar nicht so selten: Spätestens seit dem Aufkommen moderner Kryptographie basiert die Sicherheit kryptographischer Verfahren zu einem Großteil auf Einwegfunktionen, die deshalb als sicher gelten, weil ihre Umkehrung nicht in Polynomialzeit berechnet werden kann – jedenfalls bisher. Goldreich (2004, 22, Herv. i.O.) formuliert dazu pointiert: »Unfortunately, *making assertions about what can or cannot be efficiently computed is exactly what cryptography is all about*.« Die präzise und reduzierte Formulierung solcher Annahmen sind Katz und Lindell (2008, 24–25) zufolge sowohl für die Annahme selbst wichtig (je öfter diese durch ihre Anwendung getestet werde, ohne falsifiziert zu werden, desto vertrauenswürdiger werde sie), als auch für die Vergleichbarkeit kryptographischer Verfahren, wobei ein Verfahren, das auf einer vertrauenswürdigeren Annahme basiert, Vorzug zu gewähren sei. Darüber hinaus erleichtere eine klar definierte Annahme den Sicherheitsbeweis eines kryptographischen Verfahrens, indem sie eine klare Abhängigkeitskette schaffe: Ein Verfahren, das auf Annahme X basiert, ist sicher, wenn Annahme X stimmt. An dieser Stelle wird erneut das Prinzip der Modularisierung und dessen Rolle bei der Herstellung von Sicherheit sichtbar: Basiert ein kryptographisches Verfahren auf einer falsifizierten Annahme, so kann diese gegebenenfalls ausgetauscht werden, ohne das komplette Verfahren zu verändern.

Das dritte Prinzip moderner Kryptographie nach Katz und Lindell (ebd., 18) besagt schließlich, dass kryptographische Systeme über einen »rigorous proof of security« verfügen müssen. Die beiden vorherigen Prinzipien schaffen die Voraussetzungen für die Möglichkeit, einen solchen Nachweis zu erbringen (vgl. ebd., 26): Die Grundlage bildet das erste Prinzip durch die Definition dessen, was erreicht werden muss, damit ein System als sicher gilt. Das zweite Prinzip stellt eine genaue Abgrenzung der nicht-beweisbaren Anteile einer solchen Definition bereit. Ein Sicherheitsnachweis folgt daher in den meisten Fällen einem sog. »reductionist approach« gemäß der Formulierung »Given that Assumption X is true, Construction Y is secure according to the given definition« (ebd., 26).

Reduktionen

Der Vorgang der Reduktion taucht im Zusammenhang mit dem Erbringen von Nachweisen für die Sicherheit eines kryptographischen Systems mehrfach

auf, und ist auch Gegenstand der Kritik an »provable security« als Teilbereich der Kryptographie. Bereits eingeführt wurde der »reductionist approach« bei Katz und Lindell in Bezug auf die Erbringung eines Sicherheitsnachweises für kryptographische Systeme. Katz und Lindell (ebd., vi) merken im Vorwort ihres Buches an, dass sie keinen Unterschied zwischen Anwendung von und Theoriebildung für Kryptographie machen, und daher »do not separate ›applied cryptography‹ from ›provable security‹; rather, we present practical and widely-used constructions along with precise statements (and, most of the time, a proof) of what definition of security is achieved.« Der Kryptograph Neal Koblitz (2007, 976) beschreibt das Prinzip *Beweisbarer Sicherheit* folgendermaßen:

> »The idea of ›provable security‹ is to give a mathematically rigorous proof of a type of conditional guarantee of the security of a cryptographic protocol. It is *conditional* in that it typically has the form ›our protocol is immune from an attack of type X provided that the mathematical problem Y is computationally hard.‹«

Die an dieser Stelle modellhaft gegebene Sicherheitsdefinition entspricht der von Katz und Lindell. Eine gelungene Sicherheitsdefinition, führen diese an späterer Stelle weiter aus, »essentially provides a mathematical formulation of a real-world problem. If the mathematical definition does not appropriately model the real world, then the definition may be useless« (Katz/Lindell 2008, 22). Die Schwierigkeit, ein mathematisches Modell für die »real world« zu schaffen, die sich oft als widerständiger erweist als den Modellen zuträglich wäre, diskutieren Katz und Lindell (ebd., 23) anhand von zwei Szenarien. Einerseits könne die Implementierung eines mathematisch beweisbar sicheren Verfahrens in ein größeres System (z.B. in Software) andere Wege bereitstellen, mit denen das System dennoch erfolgreich angegriffen werden könne.[45] Darüber hinaus hänge im Fall von IT-Sicherheit ein mathematischer Sicherheitsbeweis davon ab, dass ein Computer ein bestimmtes Problem nicht lösen könne. »The problem is«, schreiben sie weiter, »that computation is a real-world process, and there are many different ways of computing« (ebd.,

---

45 Katz und Lindell (2008, 22–23) geben hier sog. *smart-cards* als Beispiel, also Plastikkarten, die beispielsweise als Zimmerschlüssel in Hotels verwendet werden. Diese bieten durch ihre physischen Eigenschaften eine Möglichkeit, wie der Schlüssel dennoch ausgelesen werden kann, nämlich durch die Messung der Veränderung der elektrischen Ladung der Karte bei ihrer Verwendung.

23). Daher müsse sichergestellt werden, dass die mathematische Definition von *Computation* dem entspreche, was *Computation tatsächlich* sei. Ein solcher Zugang erscheint in vielerlei Hinsicht als problematisch: Nutzungspraktiken sind vielfältig und können stark von der Designintention divergieren. Auf konkrete Anwendungsfälle hinarbeitende Antworten auf die Frage, was *Computation* sei, schreiben damit einen essentialistischen sowie instrumentellen Technikbegriff in die Überlegung ein. Katz und Lindell weiten ihre Überlegung jedoch noch weiter aus, wenn sie in diesem Zusammenhang die Überlegungen Alan Turings in seinem Aufsatz *On computable numbers, with an application to the Entscheidungsproblem* anführen, und konstatieren, dass Turing ein mathematisches Modell von *Computation* entwickelt habe, ähnlich wie es nun die Aufgabe von Kryptograph_innen sei, ein mathematisches Modell *der Welt* zu entwerfen (vgl. ebd., 23–24).

Kritik an diesem Ansatz wird auch innerhalb der kryptographischen Community geübt, wenn auch aus anderen Gründen: Neal Koblitz und Alfred Menezes haben in einigen gemeinsamen Aufsätzen die Grundannahmen *Beweisbarer Sicherheit* kritisch diskutiert (vgl. Koblitz/Menezes 2006; 2007a; 2007b). In seinem Aufsatz *The Uneasy Relationship Between Mathematics and Cryptography* fasst Koblitz die Kritik, die er gemeinsam mit Alfred Menezes an *Beweisbarer Sicherheit* geübt hat, knapp zusammen.[46] Hauptsächlich interessiert sich Koblitz dabei für die Rolle der Reduktion, allerdings mit einem anderen Schwerpunkt als Katz und Lindell: Während letztere sich hauptsächlich auf Reduktion im Sinne der Herstellung einer logischen Kette für die Erbringung eines

46 Koblitz beschreibt ebenfalls, dass seine und Menezes' Haltung innerhalb der kryptographischen Community auf reichlich Widerstand gestoßen ist. Bereits die erste Veröffentlichung der beiden zu dem Thema (vgl. Koblitz/Menezes 2007b) im *Journal of Cryptology* wurde nach einer heftigen Auseinandersetzung der Mitglieder des Herausgeber_innenteams von einer *Editor's Note* begleitet, in der die Publikation von Koblitz' und Menezes' Aufsatz gerechtfertigt wurde (vgl. Maurer 2007). Oded Goldreich, der ebenfalls Teil des Herausgeber_innenteams war, und die Publikation verhindern wollte, reagierte mit der Veröffentlichung eines Aufsatzes namens *On Post-Modern Cryptography* auf einem eprint-Server. In diesem Aufsatz, der sich besser als Schmähschrift in wissenschaftlicher Form bezeichnen lässt, kritisiert Goldreich (2012, 2) den Ansatz von Koblitz und Menezes als postmodern, denn, so formuliert er, »both post-modernism and the ›critique of rigorous analysis in Modern Cryptography‹ are reactionary (i.e., they play to the hands of the opponents of progress).« Im Verlauf des Artikels wird mehr als deutlich, dass Goldreichs Verständnis des Wortes postmodern derselbe Fehler eingeschrieben ist, der auch schon für die Science Wars kennzeichnend war: die Verkennung von Relationalismus als Relativismus.

Sicherheitsnachweises konzentrieren, und nur kurz auf die Schwierigkeit eingehen, die Welt auf ein mathematisches Modell zu reduzieren, setzt Koblitz' Kritik genau an dieser Stelle an. *Beweisbare Sicherheit*, formuliert Koblitz sein Unbehagen mit dem Term, schaffe eine Illusion von Sicherheit: Ein Aspekt dieser Illusion sei, dass (mathematisch) *Beweisbare Sicherheit* die Möglichkeit eines erfolgreichen Angriffs auf einen mathematisch-kryptographischen reduziere, was bedeute, dass jeder erfolgreiche Angriff das zugrunde liegende mathematische Problem gelöst haben müsse, wodurch ebenfalls eine Reihe weiterer Verfahren gebrochen seien. Andere Formen von Angriffen würden kategorisch ausgeschlossen (vgl. Koblitz 2007, 976–977).[47] Katz und Lindell (2008, 23) adressieren andere Formen von Angriffen nur implizit, und ihre Lösung besteht stets darin, das Modell zu verbessern. Koblitz' Kritik geht über den Ausschluss weiterer Angriffsmöglichkeiten hinaus und problematisiert auch die durch die Reduktion entstehende Kompartimentierung: Die Reduktion eines Sicherheitsproblems aus der echten Welt auf ein mathematisches Problem, und die Reduktion der Sicherheit eines kryptographischen Verfahrens auf die Bedingung, eine (bisher) unbewiesene Annahme sei korrekt, stellt für Koblitz eine Konditionalkette her. Der Begriff *provable security* sei für ein solches Verfahren »very misleading« (Koblitz 2007, 977), denn eine solche Konditionalkette sei nicht im selben Maße beweisbar wie beispielsweise der Satz des Pythagoras (der mathematisch restlos bewiesen ist), und werde oft dafür genutzt, Lai_innen zu beeindrucken und in falscher Sicherheit zu wiegen (vgl. ebd.).

Die Frage nach der Sicherheit, so lässt sich mit Koblitz' Kritik sagen, wird innerhalb der *provable security* als Teilbereich der Kryptologie mittels Reduktion entstehender Konditionalketten auf immer kleiner werdende Bereiche verschoben, aber nie zufriedenstellend geklärt. Dies ist ein Effekt der Reduktion selbst: Angriffe, die außerhalb von den modellhaft durch die Kette beschriebenen Fällen stehen, werden in den Modellen nicht mitgedacht. Darüber hinaus bauen die Glieder der Konditionalketten nicht so engmaschig logisch aufeinander auf, wie es den Anschein macht, da bei jeder Reduktion auf ein Modell

47 Dieser Einwand lässt sich als eine erneute Stärkung des Kerckhoffs'schen Prinzips begreifen, nach dem ein kryptographisches System nicht (nur) mathematisch, sondern auch praktisch nicht zu brechen sein sollte. Polemisch ließe sich Alfred North Whiteheads (1978, 39) wohl bekanntestem Zitat, »The safest general characterization of the European philosophical tradition is that it consists of a series of footnotes to Plato« folgend behaupten, die sicherste allgemeine Charakterisierung der kryptographischen Tradition Europas laute, dass sie aus einer Reihe von Fußnoten zu Kerckhoffs bestehe.

wichtige Aspekte und Widerständigkeiten der jeweils reduzierten Ebene verloren gehen. Während Katz und Lindell die mathematische Modellierung der Welt affirmieren, und davon ausgehen, dass der Hauptgrund für ein gescheitertes Sicherheitsverfahren eine ungenaue Abbildung der Welt durch das Modell sei, lässt sich das Verhältnis von Modell und Welt weitergehend problematisieren. Die oft geübte Kritik, Kryptographie und IT-Sicherheit würden versuchen, technische Lösungen für soziale Probleme zu finden, muss, um nicht erneut affirmativ mit einer noch genaueren Modellierung beantwortet zu werden, den zugrunde liegenden Sicherheitsbegriff problematisieren, dem sich bisher hauptsächlich in nachvollziehender Weise aus der Perspektive der Kryptologie genähert wurde.

Negative Sicherheit

Ob ein Verfahren, eine App, ein Programm sicher ist, um damit zur Ausgangsfrage dieses Kapitels zurückzukommen, kann also mit ja beantwortet werden, falls diese(s) eine bestimmte Leistung erfüllt: Die Einhaltung der zuvor gemachten Angaben, was wie lange und wie stark wovor geschützt werden soll. Was Sicherheit ist, wird innerhalb der Kryptologie also relational auf eine zuvor bestimmte Gefahr hin konzipiert, die in den Ausführungen zum unsicheren Kanal mit Sybille Krämer als das *störende Dritte* des technisch-postalischen Übertragungsmodells von Kommunikation bestimmt wurde. Die folgenden Überlegungen beziehen sich der Klarheit halber ausschließlich auf diese Form der verschlüsselten Kommunikation, und lassen die weiteren Anwendungsgebiete und Funktionen von Kryptographie außen vor.[48]

In der Sicherheitsforschung der letzten Jahre hat sich eine Unterscheidung verschiedener Sicherheitsbegriffe etabliert, die bisher in der vorliegenden Untersuchung nicht thematisiert wurde. Dass diese Unterscheidung nicht ganz augenfällig ist, mag auch an einer sprachlichen Ungenauigkeit liegen: Im Englischen gibt es mehrere Wörter – *security*, *safety* und *certainty* – die dem deutschen Wort *Sicherheit* entsprechen, aber unterschiedlich konnotiert

48 Weiterhin sollen die an dieser Stelle getätigten Aussagen über die strukturelle Verfasstheit kryptographischer Sicherheit nicht als großes Argument über die grundsätzliche Funktionsweise von Sicherheit in der Kryptographie im Sinne einer *strong theory*, die ungenau (genug) ist, um ein großes Feld zu organisieren, verstanden werden, denn die Sicherheitsdienste kryptographischer Verfahren sind, wie in diesem Kapitel bereits etabliert, vielfältig und nicht nur auf den Vorgang des Austauschs verschlüsselter Nachrichten zwischen zwei Parteien beschränkt.

sind und auf verschiedene Sicherheitsbegriffe verweisen. Während *certainty* ebenfalls als Gewissheit übersetzt werden kann und daher an dieser Stelle vernachlässigbar ist, soll der für die vorliegende Untersuchung relevante Unterschied von *security* und *safety* genauer betrachtet werden. Die Differenz der beiden Begriffe fällt darüber hinaus auch je nachdem, ob man technisch-naturwissenschaftlichen oder sozial- und geisteswissenschaftlichen Diskursen folgt, erneut unterschiedlich aus.

Sowohl die IT-Sicherheit, die im Englischen *IT security* heißt, als auch die Kryptologie behandelt in ihren englischsprachigen Aufsätzen zumeist *security*. Weiterhin wird in diesen, ebenso wie in anderen naturwissenschaftlich-technischen Fächern, die mit der Konstruktion und dem Erhalt von Infrastrukturen befasst sind, wenn auch nicht immer ganz trennscharf, zwischen *security* und *safety* unterschieden (vgl. Piètre-Cambacédès/Chaudet 2010). Unter dem Begriff *security* werden dabei in der Regel »malicious risks« verhandelt, wohingegen *safety* im Zusammenhang mit »purely accidental risks« verwendet wird (ebd., 59) – *security* bezeichnet das Sichern eines Systems *vor* absichtlichen Störungen, *safety* bezeichnet das Sichern des Systems *für* die Nutzer_innen oder auch die Umwelt, die durch das System nicht zu Schaden kommen sollen.[49] Angesichts dieser Unterscheidung ist es verständlich, dass sich Kryptologie, aber auch IT-Sicherheit, mit dem Ausschluss eines *störenden Dritten*, mit *security* befasst.

Sozial- und geisteswissenschaftliche Unterscheidungen von *safety* und *security* sind an verschiedenen Modi von Sicherheit interessiert, die sie auf ihre Praktiken und Rollen in gesellschaftlichen Kontexten hin untersuchen.[50] In seinem Aufsatz *Das Grundgefühl der Ordnung, das alle haben. Für einen queeren*

49 Ein Beispiel für die Diskussion von *safety* wäre die Sicherheit teilautomatisierter Herstellungsprozesse, in denen Menschen in Fabriken mit großen Industrierobotern auf engem Raum zusammenarbeiten. Damit die Sicherheit (*safety*) der menschlichen Arbeiter_innen garantiert werden kann, müssen die maschinischen Arbeiter_innen speziellen Sicherheitsprotokollen folgen, wie beispielsweise sich im Fall eines außerplanmäßigen Zwischenfalls abzuschalten.

50 Einen Überblick der Diskussion innerhalb der Sicherheitsforschung geben beispielsweise Folkers (2020) und Roe (2014). Da dieses Buch weniger an einer allgemeinen Diskussion von Sicherheitsbegriffen interessiert ist als an einer queeren Lesart von Sicherheit, werde ich diese Untersuchungen weitestgehend ausklammern, und stattdessen hauptsächlich mit Texten arbeiten, die ebenfalls Anschlusspunkte an die Queer Theory beinhalten.

Begriff von Sicherheit[51] nimmt der Philosoph und Sozialwissenschaftler Daniel Loick unter anderem eine historisierende und vergleichende Analyse negativer und positiver Sicherheit vor. Für diese Unterscheidung bezieht sich Loick auf Melanie Brazzells Arbeit zu *intersektionaler transformativer Gerechtigkeit*, einem in aktivistischen Räumen entwickelten Konzept geteilter Verantwortungsübernahme für Gewalt(-prävention). In den USA unter dem Namen *transformative justice* entwickelt, soll dieser dem Abolitionismus zugehörige Ansatz Communities dazu befähigen, Gerechtigkeit für von Gewalt betroffene marginalisierte Personen[52] zu schaffen, die von staatlichen Strukturen diskriminiert werden und sich daher nicht auf die staatliche Rechtsprechung verlassen, oder diese gar nicht erst in Anspruch nehmen können oder wollen.[53] Brazzell (2019, 19) unterscheidet in *Was macht uns wirklich sicher? Ein Toolkit zu intersektionaler transformativer Gerechtigkeit jenseits von Gefängnis und Polizei* zwischen einer liberalen Vorstellung von Sicherheit, und einer Konzeptionalisierung von Sicherheit im Sinne transformativer Gerechtigkeit. Die liberale Vorstellung von Sicherheit bestimme diese negativ, insofern sie auf die Abwesenheit konkreter Gewalttaten fokussiert sei, dadurch jedoch strukturelle Gewalt nicht in den Blick nehmen könne. Eine Konzeptionalisierung von Sicherheit im Sinne transformativer Gerechtigkeit sei positiv bestimmt, da sie keinen Schutz durch eine externe Autorität suche, sondern die Mitglieder einer Gemeinschaft selbstbestimmt ein soziales Konzept von Sicherheit für ihre Community entwerfen und umsetzen können. Brazzells Gegenüberstellung aufnehmend, unterscheidet auch Loick (2021, 267–268) zwischen *negativen* und *positiven* Konzeptionen von Sicherheit, um schließlich einen *queeren* Sicherheitsbegriff entwickeln zu können.[54] Negative Sicherheit definiert Loick als Sicherheit *vor*, und weist ihr die englische Entsprechung *security* zu, während positive Sicherheit von ihm als Sicherheit *zu* beschrieben

51 An dieser Stelle möchte ich mich bei Daniel Loick dafür bedanken, dass er mir seinen Aufsatz *Das Grundgefühl der Ordnung, das alle haben. Für einen queeren Begriff von Sicherheit* schon vor dessen Veröffentlichung zur Verfügung gestellt hat.

52 Brazzell (2019, 158) nennt unter dem Akronym QTIBPOC »Queer Trans* Inter* Black und People of Color«.

53 Brazzell (2019, 17) weist darauf hin, dass auch manche feministische Strömungen Gefahr laufen, sich kompliz_innenhaft mit einem strafenden Staat zu verhalten, und so rassistische und nationalistische Diskurse zu stärken.

54 Letzterer wird für die Analyse von Backdoors noch eine größere Rolle spielen und daher auch erst an späterer Stelle ausführlich erläutert. Auf positive Sicherheit werde ich nur am Rande eingehen, da dieses Konzept für die weiteren Ausführungen irrelevant ist.

wird, die dem englischen Wort *safety* näher stehe (vgl. ebd., 267). Loick merkt an, dass sowohl negative als auch positive Sicherheit sich zunächst als Sicherheitskritiken herausgebildet haben (vgl. ebd.), was er im weiteren Verlauf seines Aufsatzes erläutert. Negative Sicherheit sei aus einem negativen Verständnis von Freiheit entstanden, das verknüpft sei mit dem Liberalismus, der sich im 18. Jahrhundert als eine Gegenbewegung zum von Foucault beschriebenen *Sicherheitsdispositiv* entwickelte (vgl. ebd., 268–270). Der Liberalismus definierte Freiheit als den größtmöglichen Handlungsspielraum einzelner Individuen, und richtete sich damit explizit gegen die »absolutistischen Kontrollansprüche des Staates« (ebd., 267), was sich vor allem in der Formation der Wirtschaft als privatem Bereich niedergeschlagen habe (vgl. ebd., 270). Freiheit, führt Loick (ebd.) weiter aus, »wird vom Liberalismus als eine Schranke definiert, die den Bürgern die Möglichkeit verschafft, ihre privaten Interessen vom Staat und den anderen Bürgern ungestört verfolgen zu können.« Die »Schranke« ist eine treffende Formulierung, da die Rolle des Staates, wie Loick konstatiert, in Bezug auf Sicherheit nicht komplett negiert, sondern vielmehr umgedeutet werde: »Sicherheit bedeutet nicht mehr die vollständige Überwachung des gesellschaftlichen Lebens, sondern die Aufrechterhaltung der Grenzen zwischen den voneinander isolierten individuellen Handlungssphären« (ebd., 267). Die Aufgabe der Grenzsicherung komme dem Staat zu: Sicherheit bedeute in diesem Kontext, dass die eigenen, privaten Interessen mit dem staatlichen Gewaltmonopol koexistieren konnten, indem »staatliche Gewalthandlungen zu Durchsetzungsinstrumenten privater Interessen umdefiniert« (ebd., 270) wurden.[55] Basierend auf Karl Marx' Reflektionen zu Sicherheit, die dieser als Versicherung des bürgerlichen Egoismus definiert, konstatiert Loick (ebd., 271, Herv. i.O.):

> »Weil sich die Gesellschaft [als] eine Summe unverbundener Individuen darstellt, die solipsistisch ihre je eigenen Interessen verfolgen, erscheint die Andere für mich immer nur potentiell als Bedrohung meiner Freiheit (daher Sicherheit *vor*). Die xenophobe Fortifizierungslogik, die das liberale Sicherheitsdenken bis heute kennzeichnet, entspringt also einem spezifischen sozialen »Grundgefühl«, welches eine wohlgeordnete Gesellschaft als Trennung, Nichteinmischung oder Nichtansteckung imaginiert.«

55 Aus diesem Zusammenhang erklärt sich auch die historische Hauptaufgabe der Polizei als »Verteidigung der kapitalistischen Wirtschaftsordnung gegen subversive Elemente, wozu sowohl die Gefahr von Landstreicherei als auch von Arbeiteraufständen gezählt wurde« (Loick 2021, 270).

Strukturell betrachtet kann es also als Ziel eines negativen Sicherheitsbegriffs angesehen werden, eine von außen kommende Bedrohung zu verhindern, wodurch auch die Figur des *störenden Dritten* wieder auf den Plan tritt, was den negativen Sicherheitsbegriff anschlussfähig an das Sicherheitskonzept der Kryptologie macht. Dass über die 4000jährige Geschichte der Kryptologie hinweg die Rolle des Staats stets im Wandel begriffen war, tut dieser Analogie keinen Abbruch, da diesem innerhalb kryptographischer Verfahren ohnehin keine feste Rolle zukommt – vielmehr geht es um die grundsätzliche Eigenschaft der Grenzziehung, die zentral am Konzept des un/sicheren Kanals verhandelt wird, der Ein- und Ausschlüsse herstellt.[56] Um die Anschlussstelle expliziter zu formulieren: Der Sicherheitsbegriff der innerhalb des technisch-postalischen Übertragungsmodells operierenden Kryptologie lässt sich strukturell als negativer Sicherheitsbegriff bestimmen, insofern er mit Grenzregulierung und dem Ausschluss des *störenden Dritten* befasst ist. Der von Loick diagnostizierten »xenophobe[n] Fortifizierungslogik«, und dem Aspekt der »Nichtansteckung«, oder vielmehr: den Politiken der Ansteckung, wird im nun folgenden Kapitel mit einer Diskussion des Sicherheitskonzepts der IT-Sicherheit anhand von aktuellen Schadsoftware-Fallbeispielen, sowie ihrer Entstehungsgeschichte in den 1980er Jahren nachgegangen.

---

56 Darüber hinaus zieht dies nicht automatisch nach sich, dass mit kryptographischen Mitteln zu operieren immer bedeuten müsse, einem negativen Sicherheits- oder Freiheitsbegriff zu folgen: Kryptographische Mittel können in den Händen von Akteur_innen unterschiedlichster Interessen liegen und verwendet werden. So kann ein Staat mittels Kryptographie seine eigenen Interessen schützen, oder Whistleblower_innen mittels Kryptographie ihr Wissen einer Öffentlichkeit zugänglich machen und auf eine Veränderung der von ihnen angeprangerten Lage drängen. Die jeweiligen Einsatzbereiche und Taktiken, in die kryptographische Verfahren in der Praxis eingebettet sind, können die beschriebene Funktionsweise kryptographischer Sicherheit politisch rekontextualisieren, sodass mit diesen Methoden gesamtgesellschaftlich eine andere Form von Sicherheit eingefordert und hergestellt werden kann. Dennoch lässt sich anmerken, dass vor allem die deutschsprachige Diskussion um Privatheit und Datenschutz, die unmittelbar mit Kryptographie verbunden ist, stark von einem negativen Freiheitsbegriff ausgeht, was sich im Konzept des *Selbstdatenschutz* niederschlägt. Internationaler, aber von ähnlichen Grundgedanken ausgehend ist die *Cypherpunk*-Bewegung (vgl. Hughes 1993), auf die auch Rogaway (2015, 46–47) im Zuge seiner Forderung nach einer Repolitisierung der Kryptographie affirmativ rekurriert. All diesen Ansätzen ist gemein, dass sie, um Privatheit einfordern zu können, Daten als Eigentum bestimmen. Für eine Kritik dieses Konzepts siehe exemplarisch Ochs (2015) und Sevignani (2012).

3. IT-Sicherheit: Digitale Grenzaushandlungen

Im Jahr 2019 wurde in einer Online-Auktion ein Kunstwerk namens *The Persistence of Chaos* für 1,345 Millionen US-Dollar versteigert. Es handelt sich um einen vergleichsweise alten Laptop mit dem Betriebssystem *Windows XP*, der mit sechs verschiedenen Schadprogrammen aus den letzten Jahrzehnten bestückt ist: *ILOVEYOU*, *MyDoom*, *SoBig*, *DarkTequila*, *BlackEnergy* und *WannaCry* (vgl. mschf.xyz o.J.). Kreiert wurde *The Persistence of Chaos* von dem chinesischen Internetkünstler Guo O Dong in Zusammenarbeit mit einer New Yorker IT-Sicherheitsfirma namens *Deep Instinct*, die dabei behilflich war, den Laptop so zu konfigurieren, dass die Malware keinen weiteren Schaden außerhalb desselben anrichten kann (vgl. Dozier 2019). Dies erscheint, gemessen an den einzelnen Programmen, mehr als ratsam – Guo O Dong gibt auf der zum Kunstwerk gehörenden Webseite an, dass sich der durch alle sechs Programme zusammen erwirkte finanzielle Schaden auf 95 Milliarden US-Dollar belaufe (vgl. mschf.xyz o.J.). *The Persistence of Chaos* ist in mehrfacher Hinsicht ein spannendes Kunstobjekt: Zum einen stellt sich die Frage, wie es technisch überhaupt möglich ist, sechs verschiedene Malwares auf demselben Computer zu installieren, da einige der Schadprogramme die Funktionalität desselben bereits so stark beeinträchtigen dürften, dass eine normale Benutzung des Computers nicht mehr möglich sein sollte. Weiterhin sind die durch das Kunstprojekt und seine Situierung verhandelten Grenzbestimmungen bemerkenswert. Grenzbestimmungen, zu denen das Kunstwerk einlädt, und die gleichermaßen an dieses herangetragen werden, damit es als Ware zirkulieren kann. Für die nüchtern aufgeschlüsselten Bestandteile »Airgapped Samsung NC10-14GB 10.2-Inch Blue Netbook (2008), Windows XP SP3, 6 pieces of malware, power cord, restart script, malware« heißt es in den Verkaufsbedingungen:

> »The sale of malware for operational purposes is illegal in the United States. As a buyer you recognize that this work represents a potential security ha-

> zard. By submitting a bid you agree and acknowledge that you're purchasing this work as a piece of art or for academic reasons, and have no intention of disseminating any malware. Upon the conclusion of this auction and before the artwork is shipped, the computer's internet capabilities and available ports will be functionally disabled.« (Ebd.)

Die Schadsoftware muss also, den rechtlichen Rahmenbedingungen folgend, auf dem Laptop eingeschlossen und dadurch stillgestellt werden: *Dissemination* darf unter keinen Umständen geschehen – vom intendierten Eintritt in der Malware als Kunstobjekt in den Warenkreislauf einmal abgesehen. Der Laptop als »potential security hazard« evoziert damit das Bild der Büchse der Pandora, die nicht geöffnet werden darf. Um eine absichtliche Öffnung zu unterbinden und eine versehentliche Öffnung auszuschließen, wird vor der Versendung an den_die Käufer_in die Fähigkeit zur Konnektivität des Laptops zunichte gemacht. Zum einen, indem der Laptop »airgapped« versendet wird, er also nicht mehr mit dem Internet verbunden werden, und auch nicht über eine direkte Verbindung mit einem zweiten Computer mit dem Internet in Kontakt kommen kann. *Air Gaps* galten lange Zeit als Sicherheitsmechanismus, mit dem sich ungewollter Datenaustausch zuverlässig unterbinden lässt, und wurden sowohl für militärische als auch geheimdienstliche Zwecke eingesetzt, sowie in Hochsicherheitsanlagen kritischer Infrastruktur (vgl. Zetter 2014). Spätestens mit dem Erfolg von *Stuxnet*, einer Schadsoftware, die um die 2010er Jahre die Zentrifugen einer iranischen Urananreicherungsanlage beschädigte, die ebenfalls airgapped war, wurde (erneut) deutlich, dass Schadsoftware nicht nur über das Internet verbreitet werden kann, sondern auch über mobile Datenträger (vgl. ebd.). Konsequenter Weise wurden daher bei *The Persistence of Chaos* auch die Ports des Laptops zerstört, die einen Datenaustausch mittels mobiler Datenträger ermöglichen würden. Das Chaos darf also nur innerhalb des Laptops fortbestehen, dessen Grenzen als undurchlässig konfiguriert wurden.

3.1 Diskursive Ansteckungspotentiale

Die Abgrenzungen, Ein- und Ausschließungen von *The Persistence of Chaos* bieten eine Möglichkeit, den Faden der »xenophobe[n] Fortifizierungslogik«, und vor allem den Aspekt der »Nichtansteckung« (Loick 2021, 271), die kennzeichnend sind für einen negativen Sicherheitsbegriff, wieder aufzunehmen,

den Blick aber diesmal auf vernetzte Computer zu richten. Im vorangegangenen Kapitel wurde, mit Fokus auf die Verschlüsselung und Übertragung von Nachrichten, der Sicherheitsbegriff der Kryptologie als negativer Sicherheitsbegriff bestimmt. Grundlegend für diesen vom technisch-postalischen Übertragungsmodell von Kommunikation informierten Sicherheitsbegriff ist im Fall der Kryptologie vor allem die Konzeptionalisierung des unsicheren Kanals als Übertragungsmedium einer Nachricht, die auf ihrem Weg der Gefahr eines *störenden Dritten* ausgesetzt ist. Die von der Kryptologie eingesetzte Lösung dieses Problems ist die Schaffung eines sicheren Kanals durch die Verschlüsselung der Nachricht, wodurch die Gefahr des *störenden Dritten* gebannt scheint. Eine solche Konzeptionalisierung von Sicherheit bestimmt Kommunikation als Informationsaustausch, der sich im Versenden und Empfangen einer Nachricht ereignet. Kommunikation hat damit einen klar definierten Anfang und ein klar definiertes Ende, und wird innerhalb der Kryptologie weitestgehend isoliert von anderen medialen Zusammenhängen betrachtet, insofern die Regulierung der Medialität von Kryptographie innerhalb digitaler Medien die Anschlussstellen zu diesen standardisiert.

Gemäß der zuvor eingezogenen Aufteilung der Anwendungsbereiche von Kryptographie, schließt das vorliegende Kapitel mit einer Diskussion von Sicherheit vernetzter IT-Systeme abseits von Kommunikationsprozessen menschlicher Akteur_innen an, denn mit der bereits skizzierten Entstehung des ARPANET Ende der 1970er Jahre veränderte sich nicht nur die Kommunikation zwischen Menschen, sondern begannen auch Maschinen jenseits menschlicher Lesbarkeiten und Handlungen miteinander zu kommunizieren. In den 1980er Jahren ereigneten sich einige technische Weiterentwicklungen auf dem Gebiet vernetzter digitaler Medien: So wurde unter anderem mit dem Adressvergabesystem IPv4 (vgl. Postel 1981a) sowie dem Transmission Control Protocol (TCP, vgl. Postel 1981b) die Grundlage für das heutige Internet gelegt, sowie durch günstigere und effizientere Hardware Mainframe-Computer Schritt für Schritt kleiner, bis sie schließlich in den 1990er Jahren zu Personal Computern (ggf. mit Internetanschluss) wurden. Gleichzeitig entstanden die ersten Sicherheitsprobleme vernetzter Computer: Computerviren, -würmer und -trojaner, wurden (mal mehr, mal weniger) kontrolliert durch die Leitungen gesendet, sowie theoretisch aufgearbeitet (vgl. exemplarisch Cohen 1987; Spafford 1994; Spafford 1989). Die 1990er Jahre waren sowohl von dem Einzug der Personal Computer in Privathaushalte als auch von der Vernetzung derselben über das Internet gekennzeichnet (vgl. Sprenger/Engemann 2015a, 10–11). Was zunächst ein aktives Sich-Einwählen und eine kabelgebundene

Ethernetverbindung voraussetzte, wurde in den darauffolgenden Jahren zu einer kabellosen Technologie, in der alle netzwerkfähigen Geräte immer online sind, oder es zumindest qua Design[1] sein sollen. Mit dieser dauerhaften Konnektivität trat ein neues Problem auf: Der *unsichere Kanal*, auf den sich die Herstellung von Sicherheit in der Kryptologie bezieht, hat sich vervielfältigt und verstetigt – unsichere Kanäle umgeben die einzelnen Maschinen, die in einem ständigen Austausch miteinander stehen – und eine Verschlüsselung des Informationsaustauschs von Computern untereinander ist nicht gegeben. Die umfassende Vernetzung skaliert darüber hinaus Sicherheitsprobleme in vernetzten Umgebungen, wie beispielsweise Computerviren, -würmer und -trojaner auf ungekannte Ausmaße (vgl. Krämer 2008, 146), wovon nicht zuletzt *The Persistence of Chaos* zeugt. Die Eckpfeiler der zu erzählenden Geschichte der IT-Sicherheit wären allerdings mit einem Blick, der sich nur auf die technischen Entwicklungen der letzten Jahrzehnte richtet, unzureichend umrissen. Die 1980er Jahre, die sich als formative Phase für die Herausbildung der IT-Sicherheit bestimmen lassen, waren in den USA darüber hinaus maßgeblich von der Zuspitzung des Kalten Kriegs, Ronald Reagans Präsidentschaft sowie der AIDS-Krise geprägt (vgl. Deuber-Mankowsky 2017b, 15–16), die an dieser Stelle im Sinne einer Grundlage für die folgenden Ausführungen skizzenhaft dargestellt werden soll.

1981 wurde an der Westküste der USA zum ersten Mal AIDS diagnostiziert,[2] allerdings zunächst unter einem anderen Namen. Nach dem Tod von fünf, dem damaligen Wissensstand entsprechend nicht vorerkrankten Personen in Los Angeles durch eine Pneumocystis-Pneumonie, wurde in einer Veröffentlichung der Centers for Disease Control[3] (kurz: CDC) die scheinbar einzige Gemeinsamkeit der Toten genannt, und gleichsam als möglicher Auslöser der Krankheit suggestiv hervorgehoben: alle Verstorbenen waren

---

1 Diese Entwicklung wird im Spannungsfeld der Schlagwörter *ubiquitous computing* und *Internet der Dinge* verhandelt. Weiterführend dazu siehe Sprenger und Engemann (2015b).

2 Der Autor und Aktivist Theodore Kerr weist in einem Gespräch mit der Filmemacherin und Aktivistin Alexandra Juhasz darauf hin, dass das HI-Virus bereits seit Beginn des 20. Jahrhunderts in Kamerun, und bereits seit den späten 1960er Jahren in den USA zirkulierte: »There are lived experiences of HIV well before 1981, but these occur outside of discourse. Even so, a then-unnamed illness impacts individuals and communities.« Diese Phase bezeichnet Kerr treffend als »AIDS before AIDS« (Juhasz/Kerr 2020).

3 Die Centers for Disease Control sind eine Behörde des US-amerikanischen Gesundheitsministeriums.

homosexuelle Männer (vgl. Treichler 1987, 276). Noch im selben Jahr wurden die Tode weiterer homosexueller Männer an seltenen, aber normalerweise nicht tödlich verlaufenden Krankheiten auf einen Zusammenbruch des Immunsystems zurückgeführt, aufgrund dessen der Körper nicht mehr in der Lage war, sich adäquat gegen diese Infektionen zu schützen, und das diagnostizierte Syndrom mit dem Akronym *GRID* bezeichnet: *Gay-Related ImmunoDeficiency* (vgl. ebd., 277). Erst nachdem im darauffolgenden Jahr dasselbe Krankheitsbild nicht mehr ausschließlich bei homosexuellen Männern, sondern unter anderem auch bei heterosexuellen Personen diagnostiziert wurde, wurde *GRID* durch die Bezeichnung *AIDS* ersetzt: *Acquired Immune Deficiency Syndrome* (vgl. ebd.). 1984 wurde HIV als Auslöser von AIDS festgestellt (vgl. Deuber-Mankowsky 2017b, 14). Was sich an dieser Stelle durch die Knappheit der Aufzählung als eine Fortschrittsgeschichte wissenschaftlicher Objektivität missverstehen lassen könnte, ist alles andere als das. Wie Paula Treichler in ihrem Aufsatz *AIDS, homophobia and biomedical discourse. An epidemic of signification* darlegt, handelt es sich beispielsweise bei der Ersetzung von GRID durch AIDS nicht um eine Bereinigung des Wissenschaftsdiskurses von homophoben Vorurteilen, werden nicht ›unwissenschaftliche‹ Vorurteile durch ›neutrale wissenschaftliche Fakten‹ ersetzt. Vielmehr unterstreicht Treichler (1987, 266–267),

> »that no clear line can be drawn between the facticity of scientific and non-scientific (mis)conceptions. Ambiguity, homophobia, stereotyping, confusion, doublethink, them-versus-us, blame-the-victim, wishful thinking: none of these popular forms of semantic legerdemain about AIDS is absent from biomedical communication.«

Was AIDS *ist*, so Treichlers zentrales Argument, ist ein anhaltender gesellschaftlicher Aushandlungsprozess zwischen den materiellen Aspekten der Krankheit und den (möglichen) Bedeutungen, die diesen zugewiesen werden. AIDS, so schreibt sie, »with its genuine potential for global devastation – is simultaneously an epidemic of a transmissible lethal disease and an epidemic of meanings or signification« (ebd., 263–264). AIDS als *epidemic of signification*[4] zeigt sich also in den (bis heute andauernden) mannigfaltigen

---

4 Es entbehrt nicht einer gewissen Absurdität, dass das Manuskript des vorliegenden Buchs während der Covid-19-Pandemie fertiggestellt wurde, zu deren Beginn Tedros Adhanom Ghebreyesus, der Direktor der WHO, vor einer *Infodemie* warnte (vgl. The Lancet Infectious Diseases 2020). Ghebreyesus' Anliegen wird zumeist darauf bezo-

Versuchen der Sinnproduktion, die sich an den beobachtbaren Elementen der Krankheit entzünden, und von absurd wirkenden Deutungen wie AIDS sei »[a]n Andromeda strain with the transmission efficiency of the common cold« über etwas nüchternere wie »[t]he most urgent and complex public health problem facing the world today« bis hin zu homophoben Deutungen wie »[a] gay plague, probably emanating from San Francisco« oder »[t]he price paid for anal intercourse« (ebd., 264–265) reichen.

Die bisher genannten, wenigen Beispiele für homophobe Formen der Wissens- und Sinnproduktion über AIDS sind symptomatisch für die »offene Homophobie [der] konservativ-neoliberalen Politik« (Deuber-Mankowsky 2017b, 16) der Reagan-Regierung und großer Teile der Bevölkerung, die sich darüber hinaus auch in Schweigen und Passivität manifestierte: In den nicht in die Wege geleiteten Maßnahmen zum Schutz der Bevölkerung, wie beispielsweise konzentrierter Forschung über die neue Krankheit und der schnellen Entwicklung von Therapiemöglichkeiten, in der nicht erfolgten Aufklärung über die Ansteckungswege durch öffentliche Behörden, sowie in den spärlichen oder falschen Informationen über und Framings von AIDS in den Medien (vgl. Crimp 1987b; Bersani 1987, 202). Was aus der medialen Berichterstattung dafür umso deutlicher hervorging, wie Leo Bersani (ebd.), darlegt, waren »heterosexual anxieties«: Angst vor Homosexualität und homosexuellen Personen, Angst vor AIDS, und den Zusammenhängen und Ansteckungspotentialen, die diesen zugeschrieben wurden. So wurde AIDS »zu einer Strafe und Homosexualität zu einer Sünde erklärt« (Deuber-Mankowsky 2017b, 16), und es entstand eine Epidemie gewaltigen Ausmaßes. Eine ausführliche und

---

gen, die Erkenntnisse der Wissenschaft umsichtig zu kommunizieren. So sollen in medialer Berichterstattung keine Erkenntnisse aus Pre-Print-Aufsätzen, die noch nicht den gängigen wissenschaftlichen Standards zur Qualitätssicherung unterzogen wurden, als Fakten geframed werden, und den in Sozialen Netzwerken entstehenden und verbreiteten Falschinformationen wiederum mit wissenschaftlicher Klarheit und angepassten Kommunikationsstrategien begegnet werden (vgl. Zarocostas 2020). Diese Auslegung des Begriffs Infodemie setzt eine mit Neutralität gleichbedeutende Objektivität von Wissenschaft voraus und positioniert diese gleichermaßen als gesellschaftlichen Zusammenhängen äußerlich, was sich mit Treichler als unzutreffend kritisieren lässt. Einzig in der zu Beginn der Pandemie thematisierten Namensgebung des neuen Virus, bei der Bezeichnungen, die die Zugehörigkeit zu bestimmten bereits bekannten Virenstämmen wie »SARS-CoV-2« oder »CoVid-19« gegenüber ortsbezogenen Namen wie etwa »Wuhan Virus« bevorzugt wurden, um Diskriminierung zu vermeiden, wurde ein direkter Anknüpfungspunkt an Treichlers Argumentation erkennbar (vgl. Webel 2020).

in ihrer Klarheit und Stärke bewundernswerte Dokumentation, Analyse und Kritik dieser Verhältnisse stellt die 43. Ausgabe des Journals *October* aus dem Jahr 1987 mit dem Schwerpunkt *AIDS: Cultural Analysis/Cultural Activism* dar, in deren Einleitung Douglas Crimp (1987b, 13) eindringlich auf die verschiedenen Ebenen des Schweigens hinweist, die die AIDS-Krise kennzeichnen:

> »The ignorance and confusion enforced by government and the dominant media; the disenfranchisement and immiseration of many of the people thus far hardest hit by AIDS; and the psychic resistence [sic!] to confronting sex, disease, and death in a society where those subjects are largely taboo – all of these conditions must be faced by anyone doing work on AIDS.«

In diesem Zitat lässt sich auch ein weiterer Punkt ausmachen: die Zuspitzung biopolitischer Aushandlungen darüber, wessen Leben betrauerbar ist, und wessen Leben dadurch als schützenswert gilt, und wer »dem Sterben überantwortet« (Deuber-Mankowsky 2017b, 16) wird. Zu Beginn der 1980er Jahre wurde AIDS auch als »4-H disease« bezeichnet, die in erster Linie »homosexuals, heroin addicts, hemophiliacs, and Haitians« (Gilman 1987, 87) treffen würde. Diese Teile der Bevölkerung wurden somit zu sogenannten Risikogruppen erklärt, was allerdings nicht dazu führte, dass sie verstärkt geschützt wurden, sondern dass der Rest der Bevölkerung besonders *vor ihnen* geschützt werden sollte. An dieser Stelle tritt, wie Deuber-Mankowsky (2017b, 16) ausführt, die Verflechtung von Homophobie mit Rassismus, Sexismus und, wie an dieser Stelle mit Bersani (1987, 201) ergänzt werden kann, auch *class*, deutlich hervor, denn gegen diese vier (sich teilweise überschneidenden) Gruppen richteten sich gesellschaftliche Ausschlussmechanismen im Besonderen.[5] Mit Bersani (ebd., 199) lässt sich weiterhin feststellen, dass diese Gruppen nicht nur durch Passivität dem Sterben überantwortet wurden, sondern auch physischer Gewalt und Angriffen ausgesetzt waren:

> »Doctors have refused to operate on people known to be infected with the HIV virus [sic!], schools have forbidden children with AIDS to attend classes, and recently citizens of the idyllically named town of Arcadia, Florida, set fire to the house of a family with three hemophiliac children apparently infected with HIV.«

---

5 Für eine weiterführende, detaillierte Analyse der Diskursivierung von HIV, AIDS und Homosexualität in Printmedien und Fernsehen siehe Watney (1996).

Bersani führt noch einige weitere Beispiele für diese Formen von Gewalt an, die sich gegen Personen mit HIV und AIDS richten, und zeichnet die Verschiebungen nach, anhand derer die als zu einer der benannten Risikogruppen zugehörig gelesenen Personen, vor allem homosexuelle Männer, zu bereits angesteckten, infizierten und potenziell infizierenden Personen gemacht, und damit auch derselben Gewalt ausgesetzt wurden. Diese Situation reflektierend, schreibt er in seinem Aufsatz *Is the Rectum a Grave?*, der ebenfalls Teil der erwähnten Ausgabe des Journals *October* ist: »[…] given the nature of that starting point, analysis, while necessary, may also be an indefensible luxury. […] it is also important to say that, morally, the only *necessary* response to all of this is rage.« (Ebd., 200–201, Herv. i.O.) Und dennoch schreibt er, nimmt er eine Analyse vor, die ebenso eine Kritik dieser Verhältnisse ist, und gekennzeichnet von dem Wunsch nach einem besseren (Zusammen-)Leben und der Offenheit von Zukünften. Bersanis Aufsatz, die anderen Beiträge der *October*-Ausgabe, ebenso wie weitere Schriften der von HIV, AIDS und/oder der mit der AIDS-Krise einhergehenden Gewalt Betroffenen, lassen sich damit, Douglas Crimp (1987b, 7) folgend, als »cultural practices actively participating in the struggle against AIDS« begreifen.

Ein weiteres Beispiel solcher kulturellen Praktiken sind Performances und Kunstprojekte, die im Kontext der Widerstandsbewegung ACT UP (»AIDS Coalition to Unleash Power«) entstanden sind, aber auch ACT UP selbst. 1987 gegründet, war es das Ziel der Mitglieder, »›to act up‹, sich aufzulehnen, rauszugehen und im doppelten Sinn des Wortes Theater zu machen« (Deuber-Mankowsky 2017b, 14–15). Die Bewegung versteht sich selbst, wie Crimp (1987b, 7) anhand der Worte dokumentiert, mit denen die montagabendlichen Treffen eröffnet werden, als »a nonpartisan group of diverse individuals united in anger and committed to direct action to end the AIDS crisis.« Die Mitglieder von ACT UP organisierten Kunstausstellungen und Demonstrationen, führten Interventionen im öffentlichen Raum durch und leisteten Aufklärungsarbeit (vgl. Crimp 1987b), um AIDS zu politisieren und gegen die intersektional strukturierte Diskriminierung vorzugehen. Einen wichtigen Teil der Aufklärungsarbeit, aber auch der Selbstermächtigung Betroffener, machten audiovisuelle (Selbst-)Dokumentationen aus. Tragbare Videokameras mit eingebautem Videorekorder wurden ab 1983 verkauft, und wurden zum elementaren Bestandteil der ACT UP-Bewegung (vgl. Deuber-Mankowsky 2017b, 17). »Das Ziel des Video-Aktivismus war,«, führt Deuber-Mankowsky (ebd., 19) aus, »Menschen mit AIDS zu ermöglichen, sich selbst beim Machen von Geschichte zusehen zu können. Sie sollten sich nicht als

Opfer und als passiv wahrnehmen, sondern als Aktivist_innen.« So dokumentierten die Aktivist_innen, wie es war, mit HIV zu leben, an AIDS zu leiden oder zu sterben, oder geliebte Menschen mit der Krankheit zu begleiten, zu pflegen oder an diese zu verlieren, gegen die Politik und die Pharmaindustrie zu demonstrieren etc. Diese Aufnahmen richteten sich gegen »mainstream phobic portrayals of those with AIDS as pitiable victims, damnable threats, and as alone and *dying*« (Cifor/McKinney 2020, Herv. i.O.), ebenso wie gegen verbreitete Falschinformationen zu den Übertragungswegen von HIV und das Schweigen. Deuber-Mankowsky (2017b, 20) fasst pointiert zusammen: »Medien der Dokumentation, die Bild- und Tonerfassung, deren Bearbeitung und Distribution waren Teil der Politisierung von AIDS und sie waren Teil des Alltags mit AIDS.«[6]

Thematisch mit HIV und AIDS befasste medienwissenschaftliche Analysen, bemerken Marika Cifor und Cait McKinney (2020) in ihrem Aufsatz *Reclaiming HIV/AIDS in digital media studies*, konzentrieren sich zumeist auf audiovisuelle Phänomene.[7] Dies mag aufgrund der Bedeutung von Camcordern und der audiovisuellen (selbst-)dokumentarischen Praktiken der ACT UP-Bewegung nicht verwunderlich erscheinen. Dass digitale Medien in Bezug auf die AIDS-Krise oftmals als »unique format, site, or subject of study« (ebd.) von derselben getrennt betrachtet worden seien, hingegen schon – denn, so formulieren es Cifor und McKinney (ebd.), »AIDS, computing, and the Internet grew up together.« Diese Felder verbindet mehr als nur ein zeitlicher Zusammenfall: »HIV and digital media share a set of core concerns«, führen sie weiter aus, zu dem unter anderem »virality, risk, privacy, surveillance, and embodiment, to name a few« (ebd.) gehören. Die weitestgehende Absenz medienwissenschaftlicher Forschung zum Zusammenhang von AIDS und digitalen Kulturen sehen Cifor und McKinney (ebd.) als »part of a larger structural process of HIV stigma and abandonment – a cultural process that is classed, racialized, and gendered in the context of an ongoing epidemic driven by structural oppressions, from poverty to incarceration to xenophobia.« Ihren

6 Aus diesen Praktiken der (Selbst-)Dokumentation entwickelte sich schließlich, wie Deuber-Mankowsky (2017b, 14) unter Bezugnahme auf dessen Namensgeberin B. Ruby Rich darlegt, Anfang der 1990er Jahre das sogenannte *New Queer Cinema*. Für einen Überblick sowohl über die Entstehungsgeschichte als auch eine Diskussion des *New Queer Cinema* in Verschränkung mit dem Konzept des Post-Cinema, siehe Deuber-Mankowsky (2017b).

7 Cifor und McKinney (2020) betrachten für ihren Aufsatz ausschließlich Publikationen aus dem nordamerikanischen Raum.

Aufsatz verstehen Cifor und McKinney (ebd.) als einen »call to action«, dem ich gerne nachkomme, wenn auch vielleicht nicht in der Weise, die die beiden Autor_innen intendiert haben. Im Folgenden geht es weniger um Praktiken der (Selbst-)Dokumentation, des Archivs oder von Aktivismus in und mit digitalen Medien, sondern eher um eine Grundlagenarbeit für die von Cifor und McKinney eingeforderten medienwissenschaftlichen Auseinandersetzungen mit der gemeinsamen Geschichte von HIV, AIDS und digitalen Medien, oder anders formuliert: mit ihren diskursiven Ansteckungspotentialen. Das vorliegende Kapitel nimmt den Status der Übertragungen von Konzepten aus der HIV/AIDS-Forschung in die Informatik, und die damit entstandenen Politiken der Herstellung von Sicherheit in den Blick: Welcher Sicherheitsbegriff wurde in die Informatik übertragen und informiert die IT-Sicherheit? Welche Konsequenzen bringt dies mit sich?

3.2 Zwei Fallbeispiele von Ransomware

Über die Bedeutung der in den 1980er Jahren beginnenden AIDS-Krise für digitale Kulturen und ihren Zusammenhang mit IT-Sicherheit lässt sich wohl am naheliegendsten anhand von Computer*viren* nachdenken. Während Cifor und McKinney (2020) vor allem für die nordamerikanische medienkulturwissenschaftliche Publikationslandschaft diesbezüglich ein Manko diagnostizieren, wurden außerhalb derselben einige Überlegungen zu diesem Themenbereich veröffentlicht. Die umfangreichste Analyse dieser Verschränkung legt der finnische Medienwissenschaftler Jussi Parikka (2016) mit *Digital Contagions: A Media Archaeology of Computer Viruses* vor. Parikka nähert sich dem Zusammenhang von biologischen und informatischen Viren über eine medienarchäologische Herangehensweise, und bespricht nicht nur den Zusammenhang der AIDS-Krise mit der Herausbildung von IT-Sicherheit, sondern darüber hinaus auch die Diskursivierung von Computerviren als *Artificial Life* unter den Vorzeichen der Medienökologie.[8] Die australische Soziologin Deborah Lupton geht in ihrem Aufsatz *Panic computing: The viral metaphor and computer technology* (1994) darauf ein, inwiefern die Übertragung von Viralitätskonzepten, die im Zusammenhang mit der AIDS-Krise

8 Siehe dazu auch Parikkas (2005) Artikel *The Universal Viral Machine. Bits, Parasites and the Media Ecology of Network Culture.*

entstanden sind, gesellschaftliche Vorstellungen von Computernutzung prägen. Ausnahmen aus dem US-amerikanischen Raum stellen sowohl Stefan Helmreichs (2000) Aufsatz *Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism* dar, in dem Helmreich die Sprache des IT-Sicherheitsdiskurses untersucht, und sowohl Zusammenhänge zu AIDS als auch zu weiteren körperbezogenen Grenzverhandlungen[9] wie beispielsweise der des Nationalstaates und seiner Außengrenzen im Fall eines Krieges nachweist; sowie Cait McKinney und Dylan Mulvins (2019) Aufsatz *Bugs: Rethinking the History of Computing*, in dem die Rolle der Diskursivierung von Computersicherheit mittels Metaphern aus dem HIV/AIDS-Diskurs für die mit dem Einzug von Computern in Privathaushalte verbundenen Aushandlungsprozesse untersucht wird. Im deutschsprachigen Kontext finden sich Bearbeitungen des Zusammenhangs von biologischen und informatischen Viren bei Sybille Krämer (2008), die in *Medium, Bote, Übertragung: Kleine Metaphysik der Medialität* anhand des Zusammenhangs der beiden Arten von Viren sowie des Ansteckungsvorgangs Erkenntnisse über das Konzept der Übertragung entwickelt; und auch bei Brigitte Weingart (2002), die in *Ansteckende Wörter. Repräsentationen von AIDS* ebenfalls kurz auf Computerviren zu sprechen kommt. Darüber hinaus enthält auch der von Brigitte Weingart gemeinsam mit Ruth Mayer herausgegebene Sammelband *Virus! Mutationen einer Metapher* zwei Aufsätze, die die Gemeinsamkeiten und Unterschiede biologischer und informatischer Viren besprechen (vgl. Knight 2004; Schmundt 2004).

Die vorliegende Untersuchung wird sich der Verflochtenheit von HIV, AIDS und digitalen Medien ebenfalls über Computerviren nähern, aber zusätzlich das in den genannten Publikationen unbeachtet gebliebene Phänomen der *Ransomware* in den Fokus rücken, das es erlaubt, in diesen Zusammenhang auch die Entwicklung der Kryptographie mit einzuflechten. Der Name *Ransomware* bezeichnet eine Sorte Schadsoftware, »which demands a payment in exchange for a stolen functionality« (Gazet 2010, 77), die also einen gegebenen Computer in einer Weise verändert, dass er nicht mehr zu verwenden ist, oder die auf ihm gespeicherten Dateien nicht mehr intakt sind, und mittels derer versucht wird, ein Lösegeld für die Wiederherstellung des Geräts/der Daten zu erpressen. Im Folgenden wird zunächst anhand einer

---

9 Der Zusammenhang von Kriegsmetaphern, Biologie und IT-Sicherheit wird hier nicht weiter ausgeführt. Weiterführend zu Krieg und Biologie siehe Haraway (1991b), und zu Krieg, Biologie und IT-Sicherheit Parikka (2016).

der in *The Persistence of Chaos* enthaltenen Schadsoftware namens *WannaCry* die Funktionsweise von Ransomware genauer erläutert sowie Ransomware als Phänomen situiert. Anschließend wird anhand des ersten dokumentierten Falls von Ransomware aus dem Jahr 1989, dem sog. *AIDS Information Trojaner*, die Verflechtung von Ransomware mit HIV und AIDS nachgewiesen. Im weiteren Verlauf des Kapitels wird auf einen Teilbereich der Kryptologie mit dem Namen *Kryptovirologie* eingegangen, die die technische Brücke zwischen dem *AIDS Information Trojaner* und *WannaCry* bildet, aber auch die Kryptographie in die von zweierlei Arten von Viren informierten Grenzaushandlungen der IT-Sicherheit einbindet.

3.2.1 *WannaCry*

> »The more Microsoft solidifies its global monopoly, the greater the chance for a single software exploit to bring down the entire grid. The more global health networks succeed in wiping out disease, the greater the chance for a single mutant strain to cause a pandemic.« (Galloway/Thacker 2007, 17)

Im Mai 2017 beschädigte eine Cyberattacke, die unter dem Namen *WannaCry*[10] bekannt wurde, innerhalb von wenigen Stunden mindestens 200.000 Computer in über 150 Ländern (vgl. Whittaker 2019).[11] Betroffen waren ausschließlich Computer mit dem Betriebssystem *Microsoft Windows*, da *WannaCry* eine betriebssystemspezifische Sicherheitslücke ausnutzte. Im Fall eines geglückten Angriffs wurde die Festplatte verschlüsselt, sodass Nutzer_innen aus ihren eigenen Computern ausgesperrt wurden, und nur noch eine Nachricht sahen, in der sie darüber informiert wurden, dass der Zugang zu ihren Dateien durch die Zahlung eines Lösegeldes in der pseudonymen Kryptowährung *Bitcoin* wiederhergestellt werden könne – jegliche andere Interaktion mit dem Computer war nicht mehr möglich. *WannaCry* hat nicht nur die Computer von Privatpersonen getroffen, sondern auch Computernetzwerke größerer Firmen überall auf der Welt, von der *Deutschen Bahn* über *FedEx*, und auch die Mehrheit der Krankenhäuser Großbritanniens, wodurch ein mehrere Tage andauernder Engpass in der Gesundheitsversorgung entstand (vgl. Briegleb 2017; Cameron

10 Die Software hat mehrere ähnlich klingende Namen, wie beispielsweise *WanaDecrypt0r 2.0* (vgl. Briegleb 2017) oder *WanaCrypt0r* (vgl. Khomami/Solon 2017), firmiert aber zumeist unter dem sprechenden Namen *WannaCry*.

11 Die genaue Zahl lässt sich schwer bestimmen, Angaben reichen von 200.000 (vgl. Perekalin 2017) bis zu »hundreds of thousands of computers« (Whittaker 2019).

2017): Die Krankenhäuser[12] verloren nicht nur den Zugang zu Patient_innendaten, sondern waren darüber hinaus auch nicht in der Lage, Behandlungen fortzuführen, da einige medizinische Geräte, die beispielsweise zur Verabreichung von Chemotherapie verwendet werden, über ein *Windows*-basiertes Betriebssystem verfügen (vgl. Fox-Brewster 2017; Marsh 2017).

Entgegen der medialen Berichterstattung ist *WannaCry* kein Virus, sondern ein Wurm, genauer: *WannaCry* wird als *ransomware cryptoworm* klassifiziert (vgl. Chua 2017), da sich die Software autonom über das Internet verbreitet und die Schadensroutine aus der Verschlüsselung sowie einer Lösegeldforderung zusammengesetzt ist. Die Software selbst besteht aus zwei Teilen: Einem Exploit[13] und einer Verschlüsselungsvorrichtung (vgl. Perekalin 2017). Der verwendete Exploit, mit dem *WannaCry* sich über ein gegebenes Netzwerk verbreitet und andere Systeme ›infiziert‹, heißt *EternalBlue* und nutzt eine Schwachstelle im *Windows Server Message Block-Protokoll* (kurz: SMB) aus. SMB ist ein Protokoll innerhalb des Applikationsschichtennetzwerks, mit dem Dateien oder Drucker innerhalb eines lokalen Netzwerks freigegeben und geteilt werden können. Dies ist aus zwei Gründen bemerkenswert: Erstens war *EternalBlue* der NSA zum Zeitpunkt des Angriffs bereits seit mindestens fünf Jahren bekannt (vgl. Nakashima/Timberg 2017), war aber nicht publik gemacht worden, um diese Sicherheitslücke weiter ausnutzen zu können (vgl. Wong/Solon 2017).[14] Erst als eine Hacker_innengruppe, die sich als *The Shadow Brokers* bezeichnet, den Exploit von der NSA stahl, informierte die NSA *Microsoft* über die Existenz von *EternalBlue*, woraufhin *Microsoft* im März 2017 einen Patch für die Sicherheitslücke im SMB veröffentlichte (das MS17-010 security bulletin, vgl. Goodin 2017; Microsoft 2017). Genau einen Monat später, am 14. April 2017, veröffentlichten *The Shadow Brokers EternalBlue* für alle zugänglich im Internet (vgl. Wong/Solon 2017). Computer von Nutzer_innen, die *Microsofts* Sicherheitspatch nicht installiert hatten, oder

12 Tatsächlich war der Gesundheitssektor bereits vor *WannaCry* die am stärksten von Ransomware betroffene Branche (vgl. Shah/Farik 2017).

13 Als Exploit wird eine Software bezeichnet, die speziell dafür geschrieben wurde, eine bestimmte Sicherheitslücke auszunutzen.

14 *EternalBlue* fällt damit in die sog. »NOBUS«-Kategorie der NSA. Das Akronym wird mit »nobody but us« aufgelöst und bezeichnet Sicherheitslücken, von deren Existenz nur die NSA weiß, und/oder die aufgrund der benötigten finanziellen und/oder technischen Ressourcen nur die NSA ausbeuten kann, die diese nicht meldet, um sie weiterhin ausnutzen zu können (vgl. Peterson 2013).

ältere, offiziell nicht mehr unterstütze Versionen von *Microsoft Windows* verwendeten, blieben angreifbar.[15] Zweitens, da es sich bei *WannaCry*, wie bereits erwähnt, streng genommen um eine Wurmsoftware handelt. Der Unterschied von Virus und Wurm ist in diesem Zusammenhang nicht unbedeutend: Ein Computervirus ist an Programme oder Betriebssysteme ›angeheftet‹ wie an einen ›Host‹ oder ›Wirt‹, und kann nicht unabhängig von diesen laufen. Ist beispielsweise ein Computervirus in einem Word-Dokument enthalten, so richtet er keinen Schaden an, und kann sich auch nicht verbreiten, solange das Dokument nicht geöffnet wird. Ein Wurm hingegen kann sich unabhängig von einer Aktivierung durch andere Programme von einem Gerät auf ein anderes kopieren, sowie unabhängig von einem Host-Programm ausgeführt werden, was auch bedeutet, dass er unabhängig von User_inneninteraktion mit einem gegebenen Computer ist (vgl. Spafford 1989, 448). Die Nutzung von *EternalBlue* ermöglichte dem Wurmprogramm eine schnelle Verbreitung über das SMB-Protokoll innerhalb lokaler Netzwerke: Loggt sich ein mit *WannaCry* ›infizierter‹ Computer beispielsweise in einem Firmennetzwerk ein, so kann *WannaCry* sich über das SMB-Protokoll ohne weiteres Zutun verbreiten und alle anderen Computer im selben Netzwerk ›anstecken‹. *WannaCry* verbreitete sich allerdings auch über lokale Netzwerke hinaus, indem die Software zufällige IP-Adressen im Internet ansteuerte (vgl. Mackenzie 2019). Aufgrund der Verbreitungswege, aber auch der Eigenständigkeit des Wurmprogramms waren die üblicherweise empfohlenen Verhaltensweisen von User_innen zum Schutz vor Schadsoftware, wie beispielsweise keine unerwartet erhaltenen oder verdächtig aussehenden E-Mail-Anhänge zu öffnen, oder bestimmte Webseiten zu meiden, um sich vor sog. *Drive-by-Downloads*[16] zu schützen, im Fall von *WannaCry* wirkungslos. Ist ein Computer ›infiziert‹, lädt *WannaCry* die Verschlüsselungskomponente aus dem Internet herunter und beginnt damit,

15 Dies war, auch wenn es sich dabei um einen vergleichsweise geringen Anteil der befallenen Computer handelt, besonders problematisch im Fall von Microsoft Windows XP – einer älteren Windows-Version, die seit einigen Jahren offiziell nicht mehr unterstützt wird und für die es daher zunächst auch keinen Patch gab. Da Windows XP aber oftmals von Firmen genutzt wird, veröffentlichte Microsoft schlussendlich doch noch einen Patch für Windows XP (vgl. Warren 2017). Statistisch am häufigsten betroffen waren Computer mit dem Betriebssystem Windows 7 (vgl. Brandom 2017).

16 Als *Drive-by-Download* wird ein von User_innen unbemerkt ablaufender Download, meist von Schadsoftware, bezeichnet. Ein solcher Download wird durch Sicherheitslücken in Webbrowsern möglich, die von auf einer entsprechenden Webseite hinterlegten Skripten ausgenutzt werden (vgl. Hifinger 2019).

die Festplatte zu verschlüsseln. Diese Verschlüsselung kann nicht durch eine dritte Partei gebrochen werden,[17] da die Schadsoftware eine Kombination aus symmetrischer und asymmetrischer Kryptographie verwendet, was die Zahlung des Lösegelds als einziges Mittel erscheinen lässt, mit dem man im besten Fall den Zugang zu den eigenen Dateien wiedererlangt.[18]

Genauso plötzlich wie *WannaCry* sich verbreitete, kam diese Verbreitung zunächst zu einem Stopp: Der britische IT-Sicherheitsforscher Marcus Hutchins bemerkte bei der Analyse des Codes der Schadsoftware, dass diese stets vor Beginn des Verschlüsselungsvorgangs eine Domain namens https://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com ansteuerte. Hutchins fiel weiterhin auf, dass diese Domain noch nicht registriert war. Er registrierte sie, in der Hoffnung, durch eine Beobachtung der dort eintreffenden Anfragen ein genaueres Bild von der Verbreitung der Schadsoftware zu erhalten. Zu seinem eigenen Erstaunen beendete er mit der Registrierung der Domain jedoch die Ausbreitung der Schadsoftware, da diese sich, sofern sie eine Antwort von der angefragten Domain bekam, einfach abschaltete. Dies machte zwar bereits geschehene Verschlüsselungen nicht rückgängig, unterbrach aber die Verbreitung der Ransomware (vgl. Clark 2017; Hutchins 2017) – jedenfalls fürs Erste. Leicht veränderte Versionen von *WannaCry*, die nicht mehr über die Abfrage der von Hutchins registrierten Domain anzuhalten sind, sind auch heute noch im Umlauf. Zum jetzigen Zeitpunkt (Stand: Oktober 2020) führt *WannaCry* seit seinem ersten Auftauchen ungebrochen die Statistik der meistverbreiteten Ransomwares der Welt an (vgl. Chebyshev et al. 2018; Kaspersky 2020, 9; Kaspersky 2019). Wie kam es zu dieser Entwicklung?

3.2.2 Der *AIDS Information Trojaner*

Der erste dokumentierte Ransomware-Fall ereignete sich im Dezember 1989 mit einem Programm namens *AIDS Information Trojaner*.[19] Ihren Namen hat

17 Eine statistisch unbedeutende Ausnahme bildet hier das Programm *WanaKiwi*, das in manchen Fällen die Verschlüsselung rückgängig machen konnte. Voraussetzung dafür ist, dass der Computer seit Beginn des Verschlüsselungsvorgangs nicht neu gestartet wurde, da *WanaKiwi* den Arbeitsspeicher ausliest (vgl. Delpy 2017).

18 Grundsätzlich raten Polizei und Sicherheitsexpert_innen von einer Lösegeldzahlung jedoch ab (vgl. The No More Ransom Project o.J.b).

19 In manchen Publikationen wird der *AIDS Information Trojaner* lediglich als *AIDS Trojan* bezeichnet, bspw. bei Ferbrache (1992) oder Solomon (1991).

diese Schadsoftware daher, dass sie in einem interaktiven Informationsprogramm über HIV und AIDS versteckt war, das auf Floppy Disks in Umlauf gebracht wurde (vgl. Simone 2015). Die mit »AIDS Information – an Introductory Diskette Version 2.0« beschrifteten Floppy Disks der fiktiven Firma *PC Cyborg Corporation* wurden an mehrere Tausend Personen gesendet, die entweder Abonnent_innen des Magazins *PC Business World* oder Teilnehmer_innen einer WHO-Konferenz des Jahres 1988 zum Thema AIDS waren (vgl. Ferbrache 1992, 25; McKinney/Mulvin 2019, 483).[20] Mit der Installation der Software installierte der_die unwissende User_in gleichzeitig auch die Schadsoftware, die wie in einem Trojanischen Pferd in der Floppy Disk versteckt war. Nur ein Blick in die beigefügten Lizenzbedingungen — 1989 offenbar ebenso unbeliebt wie heute — hätte den Verdacht aufkommen lassen können, dass das Programm ein Scam sei: Die EULA beinhaltet mehrere unseriöse Warnungen davor, dass die Software nicht kostenfrei zu nutzen sei, listet mögliche Kosten auf und warnt potentielle Nutzer_innen davor, dass eine Installation der auf der Floppy Disk enthaltenen Software die anderen Programme des betreffenden Computers und den Computer selbst nicht unberührt lassen würde. Ein Auszug liest sich folgendermaßen:

> »You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement; your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally.« (Ferbrache 1992, 261)

Falls man sich (dennoch) dazu entschloss, die Software zu installieren, so wurde gleichzeitig die Schadsoftware sowie ein Bootcounter installiert, der in diesem Fall als Trigger einer Art Logikbombe (vgl. Gazet 2010, 78) fungierte und beim 90. Reboot des Computers die Schadensroutine auslöste. Diese besteht aus zwei Teilen: Zuerst werden alle Dateinamen auf der Festplatte verschlüsselt und anschließend eine neue Datei erstellt, um den auf der Festplatte verbliebenen Platz aufzufüllen (vgl. Solomon et al. o.J.). Nachdem dieser Prozess abgeschlossen war, wurde der_die User_in vom Computer aufgefordert, den

20 Die genaue Anzahl der versendeten Disketten variiert stark je nach der zu Rate gezogenen Publikation, was vermutlich daran liegt, dass das Ausmaß des Schadens in den frühen Publikationen, die schnell auf den Trojaner folgten, noch nicht absehbar oder zusammengetragen war. Die höchste Anzahl gibt Solomon (1991, 16) mit 20.000 Adressat_innen an.

Drucker einzuschalten, und ein Erpressungsschreiben im Stil eines Formulars für eine Lizenzerneuerung mit einer Zahlungsforderung über 189 USD für eine Jahreslizenz oder 378 USD für zeitlich unbegrenzten Zugang zur eigenen Festplatte wurde ausgedruckt (vgl. ebd.). Die Zahlung sollte an die *PC Cyborg Corporation* gesendet werden, die auch als Lizenzgeberin der Floppy Disk aufgetreten war, und ein panamaisches Postfach wurde als Zahlungsadresse angegeben (vgl. ebd.). Nur kurze Zeit nach dem Erscheinen der Lösegeldforderung versuchte die Software, verschreckte User_innen mit der Angabe auszutricksen, dass mit der Installation der Malware auf einem weiteren Computer 30 Tage Zeit erkauft werden konnten, bevor die Zahlung fällig würde – eine Prozedur, die ohne ihr Versprechen einzulösen lediglich einen weiteren Computer beschädigte (vgl. ebd.).

Die Verflechtung dieser ersten Ransomware mit HIV/AIDS erschöpft sich jedoch nicht in dem zur Tarnung des Trojaners verwendeten Programm: Höchstwahrscheinlich[21] war der Urheber des Trojaners Dr. Joseph Lewis Popp, seines Zeichens Harvard-Absolvent für Evolutionsbiologie und zur Zeit des Ransomware-Angriffs HIV/AIDS-Forscher und Consultant der WHO in Kenia (vgl. Simone 2015).[22] Zwei Wochen nach der Veröffentlichung des *AIDS Information Trojaners* erregte Popp durch sein seltsames Verhalten die Aufmerksamkeit der Behörden am Flughafen Schiphol Amsterdam, als er auf der Rückkehr von einer WHO-Konferenz in Nairobi die Worte »Dr. Popp has been poisoned« in den Koffer einer_eines Mitreisenden kratzte (vgl. ebd.). Als sein Gepäck durchsucht wurde, fand man ein Siegel der *PC Cyborg Corporation* bei ihm. Kurze Zeit später wurde Popp in Ohio festgenommen und nach Großbritannien ausgeliefert, um sich dort wegen Erpressung und Vandalismus vor Gericht zu verantworten. Allzu viel Licht ins Dunkel konnte die Verhandlung

---

21 Obwohl Popp der Einzige war, der sich aufgrund des Trojaners vor Gericht verantworten musste, bemerken Solomon, Nielson und Meldrum (o.J.) in ihrer Analyse, dass der Code des *AIDS Information Trojaners* gleichermaßen aus sehr simplen und sehr anspruchsvollen Codezeilen besteht, woraus sie folgern, der Code könne mehrere Autor_innen haben – oder mindestens mehrere Quellen, aus denen er zusammenkopiert wurde.

22 Zur Joseph Popps Beruf und Rolle bei der WHO finden sich divergierende Angaben: McKinney und Mulvin (2019, 483) schreiben, Popp sei »an anthropologist with a doctorate from Harvard who had been denied a position at the World Health Organization«; Ferbrache (1992, 27) wiederum schreibt: »Popp was a zoologist who had conducted research into animal behaviour for UNICEF and WHO, and who had examined the initial links between monkeys carrying AIDS and the human population.«

jedoch nicht bringen: Popp leugnete, mit der Floppy Disk irgendeinen Profit gemacht zu haben und beschuldigte Beschäftigte der WHO, die Direktor_innen der *PC Cyborg Corporation* zu sein. Er behauptete weiterhin, die AIDS Information Diskette 2.0 sei Teil eines geheimen Plans gewesen, Gelder für HIV/AIDS-Forschung zusammenzutragen (vgl. Wilding 1990, 2), was angesichts der Tatsache, dass hauptsächlich Organisationen, die zu HIV und AIDS forschten oder Aufklärungsarbeit leisteten, von der Schadsoftware betroffen waren, und die Forschung dadurch Rückschläge in Form von Datenverlust erlitt (vgl. Simone 2015), eher zynisch wirkt. Darüber hinaus wurde Popp nie verurteilt – der vorsitzende Richter erklärte ihn für unzurechnungsfähig, da Popp wiederholt dabei beobachtet wurde, wie er sich einen Pappkarton über den Kopf und Kondome über seine Nase stülpte, sowie sich Lockenwickler in den Bart drehte, angeblich als Schutzmaßnahme gegen Strahlung (vgl. ebd.). Nachdem die Wogen des Prozesses sich geglättet hatten, eröffnete Popp mit seiner Tochter ein Schmetterlingskonservatorium in Oneonta, NY, das auch heute noch geöffnet ist und neben Schmetterlingen auch tropische Reptilien beherbergt (vgl. Joseph L. Popp, Jr. Butterfly Conservatory o.J.; Simone 2015).

3.3 Ansteckungen/Übertragungen/Grenzaushandlungen

Der *AIDS Information Trojaner* wirft Fragen nach dem Status der Übertragungen biologischer Konzepte in die Informatik auf: In welchem Verhältnis stehen Schadprogramme und das HI-Virus, oder etwas allgemeiner: biologische Viren? Und wie wirken sich diese Übertragungen auf die Herstellung von IT-Sicherheit aus?

»Der enorme Marktwert des Virus«, schreibt Brigitte Weingart (2002, 78) in ihrem Buch *Ansteckende Wörter. Repräsentationen von AIDS*,

> »zeigt sich einerseits daran, daß der Begriff aus der Spezialisten-Domäne des wissenschaftlichen, genauer: des medizinischen (molekularbiologischen, immunologischen) Diskurses, herausgetreten und zur allgegenwärtigen Metapher geworden ist.«

So habe das Virus als Metapher »die Grenze zum Spezialdiskurs der Informationstechnologie überschritten und zirkuliert seitdem als Computervirus« (ebd.). »Erwartungsgemäß«, so schreibt Weingart (ebd., 80) weiter, »gibt es auch in der Geschichte der Computerpathologien ein Virus, dem man den Namen ›AIDS‹ gegeben hat.« Weingart (ebd.) bezieht sich an dieser Stelle auf den

AIDS Information Trojaner, gibt aber an, dass die Verknüpfung keine strukturelle sei, »denn anstelle des AIDS-Fragebogens hätte auch ein anderes Angebot stehen können.« Dieser Aussage lässt sich sowohl anhand der bereits dargelegten Verbindungen Joseph Popps zur HIV- und AIDS-Forschung, den zu großen Teilen mit AIDS-Forschung und -Aufklärung befassten Empfänger_innen, als auch basierend auf der geschilderten Funktionsweise des *AIDS Information Trojaners* widersprechen. Der Trojaner lässt sich als den Krankheitsverlauf einer HIV-Infektion bis hin zum Ausbruch von AIDS nachahmend lesen, und das nicht nur, wie Cait McKinney und Dylan Mulvin (2019, 484) in ihrem Aufsatz *Bugs: Rethinking the History of Computing* spitz bemerken, mit einem »particularly distanced squint«: Angefangen bei der Infektion/Installation, über die ihr folgende symptomlose Latenzperiode, wie sie nach einer HIV-Infektion auftritt, die ihr Äquivalent in der Zeit bis zum 90. Reboot des Computers findet. Schlussendlich kommt es zum Auftreten von Symptomen, entweder in der Form von verschiedenen Krankheiten, die zusammengenommen das Krankheitsbild AIDS ausmachen, oder durch die ablaufende Schadensroutine. Ein entscheidender Aspekt, in dem die Verbindung nicht aufgeht, ist die Frage nach Intentionalität der jeweiligen Phänomene: Während der *AIDS Information Trojaner* oder andere Computerviren oder -würmer von Menschen geschrieben und in Umlauf gebracht werden, und sich eine Intention feststellen lässt, trifft dies auf HIV/AIDS nicht zu (vgl. Helmreich 2000, 482). Es lassen sich, abgesehen von dieser Einschränkung, also sowohl personelle als auch strukturelle Verbindungen zwischen HIV, AIDS und dem *AIDS Information Trojaner* herstellen. Eine weitere Verbindung, die sie als »Verwicklung der Ansteckungsverfahren« bezeichnet, liefert Weingart (2002, 80) selbst:

> »Wer jede x-beliebige Diskette nicht als per se mit Vorsicht zu behandelnden ›Fremdkörper‹ erachtet, sondern in den ›intimen Öffnungen‹ seines Computers zuläßt, ist beim ersten Test – auf ›gesundes Mißtrauen‹ – schon durchgefallen. Er/sie hat sich mit dieser Fahrlässigkeit gewissermaßen schon in die ›Risikogruppe‹ katapultiert.«

Bereits in diesem kurzen Zitat – stets in Anführungszeichen geschrieben, um uneigentliche Rede zu markieren[23] – ist eine Fülle von Ausdrücken enthalten,

23 Weingart (2002, 11–12) thematisiert die Verwendung von vorsichtiger, uneigentlicher Rede mehrfach in ihrem Buch, und bezeichnet diese Verwendung von Anführungszeichen als Markierung derselben mit Hubert Fichte als »Zungenpräser«: »›Zungenpräser‹ kann auch als Metapher für ›diskursive Verantwortung‹ interpretiert werden,

die den IT-Sicherheitsdiskurs bis heute prägende Konzepte ansprechen, und die am öffentlichen Diskurs um HIV und AIDS orientiert sind. Interessant ist darüber hinaus, dass Weingart eine Übertragung vornimmt: Es handelt sich beim *AIDS Information Trojaner* keineswegs um einen Computervirus, sondern, wie der Name schon sagt, um einen Trojaner – was Weingart (ebd.) auch kurz bemerkt, nur um dann darüber hinwegzugehen, indem sie schreibt, dass man von dem Trojaner »mit der Infektion durch ein Computervirus bestraft« werde. Auf technischer Ebene ist diese Bemerkung inkorrekt: Was Weingart als Virus identifiziert, ist vielmehr die Schadensroutine, die die Dateinamen mit einer monoalphabetischen Substitutionschiffre verschlüsselt (vgl. Gazet 2010, 78). Über Eigenschaften von Computerviren, wie sie in der Informatik definiert werden (vgl. Cohen 1987), verfügt der *AIDS Information Trojaner* keine. Weingart ist mit dieser Sorte Übertragung jedoch nicht allein: Mit einiger Regelmäßigkeit werden die Begriffe Virus und Wurm in medienkulturwissenschaftlichen Texten, aber auch in Zeitungsartikeln durcheinandergebracht oder synonym verwendet. So bezeichnet im Sammelband *Virus! Mutationen einer Metapher* bspw. Hilmar Schmundt (2004, 170) den *AIDS Information Trojaner* als »AIDS-Virus«. Im selben Band schreibt Peter Knight (2004, 196, Herv. MS) über den ILOVEYOU-Wurm: »Beim Ausbruch des ILOVEYOU-*Virus* wurden die Netzwerk-Server zwar mit E-Mails verstopft, die der *Wurm* massenhaft generiert hatte […].« Der Soziologe Andrew Ross (1991) schreibt in seinem Essay *Hacking Away At The Counterculture* abwechselnd über den »Morris virus« und den »Morris worm«. Es würden sich noch zahlreiche weitere Beispiele für diese Verwechselung anbringen lassen. Von größerem Interesse für die folgenden Betrachtungen, als den genannten Autor_innen etwaige Ungenauigkeiten nachzuweisen, ist die Frage, wie und weshalb diese Gleichsetzung

---

die gleichermaßen auf diejenigen übergeht, die eine Analyse des Diskurses über AIDS unternehmen (als Anweisung, ein Blatt vor den Mund zu nehmen). Auch wenn Anführungszeichen, diese ›Präservative des *speech act*‹, immerhin markieren, daß man bezüglich der Worte wählerisch ist, reichen sie kaum aus, um Diskurse abzusichern, *safer text* zu produzieren. […] Das gilt auch und erst recht für die ›ansteckenden Wörter‹, die im Diskurs über AIDS zirkulieren und deren epidemische Verbreitung ebenso zum Gegenstand dieses Buches gehört wie die Versuche ihrer Kontrolle.« Auch in der vorliegenden Publikation habe ich bisher zumeist ähnliche Vorsichtsmaßnahmen verwendet, und mich etwa bemüht, in den technischen Beschreibungen so wenig wie möglich umgangssprachlich zu schreiben. Dennoch lässt sich mit Donna Haraways Konzept der *Trope* berechtigter Zweifel an diesen Vorsichtsmaßnahmen anbringen, die den Versuch begleiten, Viralität explizierend kontrollieren zu wollen.

von Ransomware, Wurm und Virus möglich wird (und sich in die Texte einschleicht). Eine naheliegende Vermutung ist, dass diese Phänomene über Gemeinsamkeiten mit Computerviren verfügen, die im Folgenden untersucht werden sollen.

3.3.1 Metaphorische Grenzaushandlungen

Liest man über *WannaCry*, den *AIDS Information Trojaner*, oder andere Schadsoftware, so fällt auf, dass die Sprache, die zur Beschreibung dieser Phänomene genutzt wird, durchzogen ist von Elementen des uneigentlichen Sprechens, die sich größtenteils als Alltagssprache naturalisiert haben, aber bei genauerem Hinhören doch herausstechen: Computer*viren infizieren*, oder *greifen an*, Verschlüsselung wird *gebrochen*, in gehackte Systeme wurde *eingebrochen* – überall scheint die Sprache, mit der Phänomene aus dem Bereich der IT-Sicherheit beschrieben werden, von Metaphern der Grenzaushandlungen durchsetzt zu sein. Der Begriff der Metapher ist, so ließe sich sagen, in der Theoriebildung überbesetzt.[24] »[E]ine ausführliche Aufarbeitung metaphorologischer Positionen«, bemerkt Christina Brandt (2004, 28) dazu in *Metapher*

24 Medienwissenschaftliche Arbeiten, die sich dezidiert mit Metaphern auseinandersetzen, sind beispielsweise Marianne van den Boomens (2014) *Transcoding the Digital: How Metaphors Matter in New Media*, Matthias Bickenbachs und Harun Mayes (2009) *Metapher Internet. Literarische Bildung und Surfen*, sowie Georg Christoph Tholens (2002) *Die Zäsur der Medien. Kulturphilosophische Konturen*. Bei Tholen lassen sich durchaus Anknüpfungspunkte an Krämer finden, dennoch weist sein Anliegen, das Verhältnis von Medien und Menschen zu bestimmen, in eine andere Richtung als das der vorliegenden Publikation, und wird daher nicht eingebunden. Während Bickenbach/Maye und van den Boomen extrem detaillierte Überlegungen zum Verhältnis von Metaphern und den von ihnen untersuchten Medien präsentieren, verzichtet die vorliegende Publikation auf eine Einbindung ihrer Texte, da diese dazu tendieren, die von ihnen untersuchten Phänomene in der exakten Einteilung in bestimmte metaphorische Phänomene stillzustellen. Der vorliegenden Publikation geht es genau nicht um die Herstellung von festen Kategorisierungen, sondern um die Nachzeichnung der Ansteckungspotentiale von Metaphern, die mit Krämer, Treichler und Haraway als andauernde Aushandlungsprozesse begriffen werden sollen. Als weiterführende Grundlagentexte zur Metapher sind unter anderem Hans Blumenbergs (1997) begriffsgeschichtliche Studie *Paradigmen zu einer Metaphorologie*, George Lakoffs und Mark Johnsons (1996) neurolinguistische Untersuchung *Metaphors We Live By*, sowie die philosophischen Ausführungen *Models and Metaphors: Studies in Language and Philosophy* von Max Black (1962), sowie Jacques Derridas (1983) Ausführungen zur Metapher in *Grammatologie* (auf die sich auch Sybille Krämer bezieht) zu nennen.

und Experiment. Von der Virusforschung zum genetischen Code, wäre »selbst ein Unternehmen in Buchumfang.« Auch die vorliegende Untersuchung möchte, Brandts Geste folgend, eine solche Aufarbeitung an dieser Stelle nicht leisten, da sie dem Erkenntnisinteresse dieser Untersuchung nur bedingt zuträglich wäre. Ein lockerer Metaphernbegriff, der eher in die Richtung von Donna Haraways bereits eingeführtem Konzept der *Trope* strebt, ist für die folgenden Betrachtungen ausreichend und soll im Hinblick auf das Erkenntnisinteresse dieser Untersuchung kurz umrissen werden.

Das in den deutschen Sprachgebrauch überführte Wort *Metapher* stammt vom griechischen Wort *metaphorā* ab, das mit »Übertragung« übersetzt werden kann (Kluge 2012a), und befindet sich damit bereits an einem neuralgischen Punkt für medientheoretische Überlegungen. Mit Sybille Krämer (2003, 84) wurden bereits in Kapitel 2 *Übertragung* und *Inkorporation* als Eigenschaften von Medien eingeführt. Das Zusammenwirken beider Begriffe ermöglicht es, auf die von Krämer (ebd., 84–85, Herv. MS) ausgemachte »Gretchenfrage« der Medientheorie, ob Medien Sinn erzeugen oder vermitteln, zu antworten, dass »Medien im Akt der *Übertragung* dasjenige, was sie übertragen, zugleich mitbedingen und prägen.« In der Übertragung liegt also die Konstitutionsleistung von Medien begründet. An dieser Stelle lohnt es sich, noch mal einen Schritt zurückzugehen: »Der für die Medientheorie relevante Begriff der ›Übertragung‹«, schreibt Krämer (ebd., 84), »kann am Vorbild jener Art von Übertragung gewonnen werden, welche für die Metapher (meta-phora) grundlegend ist.« Umgekehrt bedeutet dies für die Metapher, dass diese eine Übertragung vornimmt, und damit über ein generatives Moment verfügt, sowie zwei voneinander getrennte Bereiche voraussetzt, zwischen denen eine solche Übertragung stattfinden kann. Wie bereits in der Einleitung dargelegt, ist die vorliegende Publikation daran interessiert, die Übertragungsprozesse von Konzepten und Begriffen zwischen wissenschaftlichen Sphären nachzuvollziehen, deren Wissensproduktion unterschiedlichen Rationalitäten folgt. Deuber-Mankowsky (2020, 135) folgend wurden diese Rationalitäten als von unterschiedlichen »Regeln und Prozessen« gekennzeichnet bestimmt, und die jeweiligen Wissensbestände damit als unterschiedlichen Ordnungen angehörend. Für das vorliegende Material bedeutet dies: Bei der Übertragung des Konzepts *Virus* aus der Immunologie in den Zusammenhang der Informatik wird nicht einfach nur ein dort angesiedeltes Phänomen erläutert, sondern entsteht es erst in und durch metaphorische Übertragung. Im Fokus steht also die Medialität von Metaphern, die sich in einer Art fraktaler Baumstruktur ebenfalls durch Übertragung und Inkorporation auszeichnet. Der Aspekt der

Inkorporation, dem Krämer ebenfalls Eigenschaften zuschreibt, die über ein bloßes *Ver*körpern hinausgehen, lässt sich mit Haraways Konzept der *trope* und dem Ausdruck *materiell-semiotisch* noch weiter stärken: Zwar sind Metaphern bei Haraway »tools and tropes« (Haraway 2018, 39), und Wörter »thick, living, physical objects that do unexpected things« (Haraway 1997, 125), aber die Phänomene, die sie bezeichnen, werden nicht einfach nur in sprachlichen Zusammenhängen verwoben, sondern arbeiten an diesen Zusammenhängen mit. So schreibt Haraway (2018, 97) im Zuge ihrer Betrachtungen der *OncoMouse*:

> »The collapse of metaphor and materiality is a question not of ideology but of modes of practice among humans and nonhumans that configure the world – materially and semiotically – in terms of some objects and boundaries and not others.«

Eine Lesart Haraways, die den Prozess der Herstellung von Wissen nur auf die Rolle von Sprache konzentriert, würde ihrem Einsatz nicht gerecht werden. An der Herstellung von Wissen ist also nicht nur Sprache mit ihrer Körperlichkeit beteiligt, sondern auch die Materialitäten der beschriebenen Objekte, die daran mitarbeiten, wie sie beschrieben werden können, und Sprache eben nicht nur im Sinne einer passiven Verkörperung erdulden. Die Konsequenz, die sich daraus ableitet, formuliert Haraway (ebd., 39) folgendermaßen: »The point is to learn to remember that we might have been otherwise, and might yet be, as a matter of embodied fact.« Bevor es im nächsten Kapitel um die spekulativen Zukünfte gehen kann, die Haraways Konzept des Materiell-Semiotischen eröffnen, soll allerdings nun endlich ein Überblick über die Geschichte und den Status Quo der IT-Sicherheit gegeben werden.

3.3.2 Zur Medialität von Viren und Würmern

1984 veröffentlichte der Informatiker Fred Cohen[25] einen Aufsatz, in dem er »a major computer security problem called a virus« (Cohen 1987, 22)[26] vorstellt.

---

25 Die Bezeichnung der geschriebenen Software als Virus geht auf Cohens Mentor Len Adleman zurück (vgl. Cohen 1987, 31), der den Leser_innen hier bereits als einer der drei Erfinder des ersten auf Diffies und Hellmans Konzept aufbauendem asymmetrischen Verschlüsselungsverfahren RSA bekannt ist, aber dies soll nur am Rande bemerkt sein.

26 In dieser Publikation wird die 1987 im Journal *Computers & Security* veröffentlichte Version zitiert.

»The virus is interesting«, schreibt Cohen (ebd.) weiter, »because of its ability to attach itself to other programs and cause them to become viruses as well.« Ein weiterer technischer Faktor, der Computerviren interessant macht, ist die zum damaligen Zeitpunkt noch weit verbreitete Nutzung von Time-Sharing-Computern durch jeweils mehrere User_innen. Die bisher implementierten Sicherheitsmechanismen dieser Systeme konzentrierten sich auf das Verhindern von »illicit dissemination of information« (ebd.): Es wurden für alle Nutzer_innen passwortgeschützte, eigene Bereiche angelegt, innerhalb derer sie ihre Dateien speichern konnten, was bereits mit Paul Ferdinand Siegert (2008, 191) als eine erste Form der Herstellung von Sicherheit als *access control* eingeführt wurde. Computerviren setzten an der Kehrseite dieses Phänomens an, denn, wie Cohen (1987, 22, Herv. MS) ausführt, »little work has been done in the area of keeping information *entering* an area from causing damage.« Die Definition des neuen Sicherheitsproblems lautet folgendermaßen:

> »We define a computer ›virus‹ as a program that can ›infect"[27] other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows.« (Ebd., 23)

Computerviren sind also Programme, die andere Programme infizieren, anstecken, das heißt: sich auf andere Programm *übertragen*, indem sie diese umschreiben. Der Begriff Virus als Bezeichnung für ein biologisches Phänomen kommt aus dem Lateinischen und bedeutet so viel wie *Saft* oder *Gift* (vgl. Kluge 2012b). Auch die Infektion hat ihre Wurzeln im Lateinischen, genauer dem lateinischen Verb *inficere*, das mit »vergiften, verpesten, beflecken« übersetzt wird (Krämer 2008, 138). Auf einen umfassenden wissenschaftsgeschichtlichen Überblick, wie das Virus zum Gegenstand der Bakteriologie und Medizin wurde, wird an dieser Stelle zugunsten der Stringenz der Argumentation verzichtet,[28] die lediglich das Wissen um Viren als ansteckende Elemente, durch die Infektionskrankheiten übertragen werden, voraussetzt. Durch die von ihnen geleistete Übertragung sind Viren auch medienwissenschaftlich ein

---

27 Der Virus und seine Eigenschaft der Infektion, die an dieser Stelle noch in Anführungszeichen geschrieben sind, werden im Verlauf des Aufsatzes von diesen befreit und damit im Sprachgebrauch naturalisiert.

28 Für einen solchen Überblick siehe exemplarisch Brandt (2004, 55–103).

interessantes Phänomen. So widmet auch Sybille Krämer biologischen und informatischen Viren ein Unterkapitel in *Medium, Bote, Übertragung*. »Wenn von ›Computerviren‹ gesprochen wird«, schreibt sie, »scheint hier das medizinische Vokabular auf äußerste Weise ins Metaphorische gedehnt« (ebd., 145). Dennoch betrachtet Krämer (ebd., 158) Computerviren und biologische Viren im Hinblick auf ihre Gemeinsamkeiten, um anhand dieser beider Viren ein Konzept dessen zu entwickeln, was sie als »Übertragen durch Ansteckung« ausmacht, und was sich in Anlehnung an den Begriff Medialität als *Viralität* beschrieben ließe. Die Übertragung durch Ansteckung umfasst Krämer zufolge fünf Punkte, die im Folgenden spezifisch im Hinblick auf Computerviren diskutiert werden: Somatizität, Heterogenität, Nichtreziprozität/Unidirektionalität, Umschrift und Gewaltsamkeit (vgl. ebd.).[29]

Unter *Somatizität* versteht Krämer (ebd.), dass die Übertragung durch Ansteckung ein körperliches Phänomen ist, insofern sie Körper ebenso wie Kontakt zwischen diesen voraussetzt. »To talk of viruses«, schreibt auch Parikka (2016, 94), »is to talk of embodiment, but not merely involving human bodies.« Für Computerviren bedeutet dies, dass Computer als Körper gedacht und konzipiert werden, was, wie er darlegt, bereits in den 1950er Jahren mit der Analogie von CPU und Gehirn begonnen hat (vgl. ebd., 111), aber auch, dass einzelne Programme innerhalb desselben Computers analog zu Körpern verstanden werden können (vgl. Ferbrache 1992, 44). Das bekannte UNIX-Diktum »Everything is a file«[30] ließe sich als »Everything is a body« neu formulieren, insofern Computerviren innerhalb ein und desselben Computers von Programm zu Programm übertragen werden können.

Unter dem Punkt *Heterogenität* erläutert Krämer (2008, 158), dass Ansteckungen nur zwischen »äußerst differierenden Systemen« geschehen können, »sei diese Differenz nun beschrieben als eine zwischen Eigenem und Fremdem, Gesundem und Krankem […].« Dies begründet Krämer in der Immunisierung, mit der Ansteckung verhindert werden kann, indem die

29 Die Diskussion um die Ähnlichkeit von Computerviren und biologischen Viren innerhalb der Informatik bezieht sich eher darauf, wie stark die Analogie zu biologischen Viren tatsächlich trägt, indem versucht wird, die biologischen Vorgänge exakt mit den informatischen zusammenzubringen (vgl. exemplarisch Ferbrache 1992; Forrest et al. 1997; Spafford 1989). Eine Diskussion der Ähnlichkeit der Medialität von Computerviren und biologischen Viren erscheint an dieser Stelle zielführender.

30 »Everything is a file« weist darauf hin, dass sowohl gespeicherte Dateien wie Bilder, Texte oder Musik als auch die Programme, mit denen sie angezeigt werden, Text*dateien* sind, und gleichermaßen bearbeitet werden können.

Unterschiede zwischen dem infizierten und dem noch nicht infizierten System aufgehoben werden. Dies trifft auf Computerviren nur bedingt zu, denn Viren, die beispielsweise innerhalb des *Microsoft Windows*-Betriebssystems funktionieren, tun dies nicht auf UNIX-basierten Systemen. Die Systeme dürfen also nicht so heterogen sein, dass die zwischen ihnen ausgetauschten Daten nicht auf beiden Systemen auch *ausgeführt* werden können, eine gewisse gemeinsame Sprache muss gegeben sein.

Der Aspekt der Heterogenität ist direkt anschlussfähig an den der *Umschrift*: Verfügen differente Systeme über eine gemeinsame Sprache, oder vielmehr über einen gemeinsamen Code, so können Viren zwischen ihnen übertragen werden, und sich in das noch nicht infizierte System einschreiben, es also umschreiben. Die Übertragung durch Viren, so formuliert Krämer (ebd., 159), ist »mit Prozessen der Informationsverarbeitung verbunden«. Bei der Informationsverarbeitung heterogener Systeme schließen auch Galloway und Thacker (2007, 86) an: »What counts is not that the host is a ›bacterium,‹ an ›animal,‹ or a ›human.‹ What counts is the code – the number of the animal, or better, the numerology of the animal.« Auch wenn bereits in Kapitel 2 darauf hingewiesen wurde, dass die Ausdeutung dieses Codes als kryptographisch (vgl. ebd.) unzutreffend ist, und das Element des Satanistisch-Okkulten, das in der Anspielung auf die Numerologie/Zahl des Tieres aufscheint, in der vorliegenden Publikation nicht mitgetragen wird, so lässt sich dennoch nicht abstreiten, dass Übertragung durch Ansteckung, und damit Viren die – informatisch ausgedrückt – Interoperabilität differenter Systeme voraussetzen. Ein Beispiel dafür ist der gelungene Hack einer DNA-Sequenziermaschine, bei dem mit einem in DNA codierten Computervirus im Vorgang der Sequenzierung die Maschine infiziert wurde (vgl. Fischer 2017; Ney et al. 2017).

Der Aspekt der *Nichtreziprozität/Unidirektionalität* ist spannend, weil er sich bei Computerviren einerseits auf den technischen Vorgang beziehen lässt: Die Weitergabe des Virus geschieht nur in eine Richtung zur selben Zeit, d.h. ein Computervirus kann nur ein anderes Programm mit diesem infizieren, aber nicht gleichzeitig sich selbst, da es bereits infiziert ist. Andererseits kann die Unidirektionalität mit McKinney und Mulvin auch auf das diskursive Ansteckungspotential zwischen Informatik und HIV/AIDS bezogen werden: »[T]he homology between computing and HIV is asymmetrical. Examples of HIV used in computer network discourses are abundant, while we found only a small set of examples of AIDS activists responding to or refracting this metaphor.« (McKinney/Mulvin 2019, 482)

Damit bleibt als letzter Aspekt der der *Gewaltsamkeit* von Übertragung durch Ansteckung, den Krämer (2008, 159) einerseits im invasiven und passivierenden Moment der Ansteckung ausmacht – wer oder was angesteckt wird, dem_der widerfahre etwas, das größtenteils nicht von ihm_ihr kontrolliert werden könne – und andererseits in den Präventions- oder Gegenmaßnahmen wie der Immunisierung oder etwa der Quarantäne.

Bevor im nächsten Unterkapitel genauer auf die Immunisierung eingegangen wird, soll der Blick noch einmal kurz auf Computerwürmer gerichtet werden, also auf Programme, die sich autonom und ohne dabei andere Programme zu verändern durch ein Netzwerk bewegen. Während Computerviren explizit als Sicherheits*problem* eingeführt wurden, was Handlungsbedarf impliziert, so bespricht Cohen (1987, 22) Würmer eher wohlwollend: Über den Xerox Wurm beispielsweise schreibt er, dieser habe »accidentally« zu einem *Denial of Service*, also einer Überlastung des Netzwerks geführt. Diese Gleichgültigkeit gegenüber Würmern lässt sich einerseits als strategisch interpretieren, schließlich geht es um die Absteckung des neuen Phänomens, und den damit verbundenen Expertenstatus bezüglich notwendiger Sicherheitsmaßnahmen für das neue Problem, und den daraus erwachsenden Möglichkeiten finanzieller Förderung der Forschung. Aus heutiger Perspektive lässt sich diese Haltung allerdings auch mit Parikka (2016, 20) darauf zurückführen, dass die Ursprünge von Würmern »in the needs of network computing in general« liegen: Manche sich wiederholenden Abläufe, die beispielsweise zur Systempflege notwendig sind, wurden als weitestgehend autonom agierende Programme automatisiert, die damit nicht als »anomalies in the simple sense of the word but [as] part and parcel of the emergence of network systems« (ebd.) einzustufen sind. Für Würmer und für Viren gilt damit eine Ambiguität, die in den nächsten Jahrzehnten sukzessive vereindeutigt werden sollte: »[E]ssentially the same program can be defined as a utility program in one context and as a malware program in another.« (Ebd.) Festzuhalten ist an dieser Stelle zunächst, dass Viren und Würmer nicht als vernetzten Systemen äußerliche Störfaktoren begriffen,[31] sondern vielmehr als »a phenomenon of time-

31 In seinem Aufsatz *The Universal Viral Machine. Bits, Parasites and the Media Ecology of Network Culture* macht Parikka (2005) dasselbe Argument stark, jedoch nicht aus einer medienarchäologischen, sondern aus einer medienökologischen Perspektive. Eine affirmative Verwendung des Begriffs *environment* ist jedoch aufgrund der Verstrickung dieses Konzepts mit der Politik des Nationalsozialismus mit Sprenger (2019) kritisch neu zu evaluieren.

sharing, networking, and, broadly speaking, connectivity« (ebd.) im Allgemeinen betrachtet werden müssen.[32] Weiterhin überschneiden sich die Phänomene Computerviren und -würmer also einerseits in der Ambiguität ihrer Nutzungspraktiken, sowie in ihren ähnlichen Verbreitungsdynamiken: Von den mit Krämer ausgeführten Kriterien für Viralität teilen sie Somatizität, Heterogenität, Unidirektionalität und Gewaltsamkeit, während Umschrift[33] bei Würmern nur bedingt gegeben ist. Diese Überschneidungen beantworten die eingangs aufgeworfene Frage, wie die synonyme Verwendung oder unabsichtliche Verwechselung von Computerviren und -würmern möglich wird.

Die Ambiguität von Computerviren stellt die noch verhältnismäßig junge IT-Sicherheit vor ein nicht zu unterschätzendes Problem, das Cohen (1987, 34) nach einigen Überlegungen zur Prävention, aber auch Reparatur von durch Computerviren entstandenen Schäden, in seinen abschließenden Bemerkungen zur Herstellung von Sicherheit in vernetzten Systemen thematisiert:

> »To be perfectly secure against viral attacks, a system must protect against incoming information flow, while to be secure against leakage of information a system must protect against outgoing information flow. In order for systems to allow sharing, there must be some information flow. It is therefore the major conclusion of this paper that the goals of sharing in a general purpose multilevel security system may be in such direct opposition to the goals of viral security as to make their reconciliation and coexistence impossible.«

Wie können vernetzte Systeme, mit ihren körperlichen Qualitäten, vor einem Phänomen geschützt werden, das in denselben begründet liegt? Wie kann Informationsverarbeitung vor dem Missbrauch ihrer zentralen Funktionselemente, dem Lesen und Um/Schreiben, geschützt werden? Und wie wird dieser definiert, also, was ist normale und nicht-normale Computernutzung?

---

32 Eine solche Lesart steht Konzeptualisierungen von Computerviren als terroristischen Entitäten, die ein geschlossenes System infiltrieren oder von außen bedrohen, und damit der Gleichsetzung von Computernetzwerken mit Nationalstaaten, wie sie beispielsweise das FBI in den 1990er veranschlagte (vgl. Helmreich 2000, 485), diametral entgegen.

33 Ob Umschrift als eine Eigenschaft von Computerwürmern definiert wird, oder nicht, hängt von der eingenommenen Perspektive ab. Würmer schreiben im Gegensatz zu Viren keine Programme um, um sich in diese hineinzuschreiben. Aus der Perspektive, dass alle Aktionen in digitalen Medien *schriftliche* Operationen sind, nimmt der Wurm sehr wohl eine Umschrift von Daten auf der Festplatte eines Computers vor.

Die von Cohen diagnostizierte Unvereinbarkeit von vernetzten Systemen, die Informationsaustausch erlauben, mit (Sicherheit vor) Computerviren scheint mit der Formulierung, »reconciliation and coexistence« seien unmöglich, zunächst für eine Unterbrechung des Informationsaustauschs zu plädieren, und damit in die Richtung der von Loick (2021, 271) benannten »Fortifizierungslogik« eines negativen Sicherheitsbegriffs zu zeigen. Dies ist offensichtlich nicht passiert – aber was stattdessen?

3.3.3 Liberale Abwehrmechanismen

Wie der Soziologe Andrew Ross in seinem Aufsatz *Hacking Away at the Counterculture* ausführt, nahm die Verstrickung von biologischen Viren und computerbezogenen Phänomenen in der medialen Berichterstattung und damit auch der breiten Öffentlichkeit Ende der 1980er Jahre ausgerechnet mit einem Computer*wurm* Fahrt auf: Der sogenannte *Morris Worm*, benannt nach seinem Autor Robert Morris,[34] verbreitete sich Anfang November 1988 über das Internet und ARPANET auf ungefähr 6000 Computer (vgl. Ross 1991, 75). Dies ist, folgt man der Schätzung in Eugene Spaffords (1989, 446) Aufsatz *The Internet Worm Incident*, dass ungefähr 60.000 Computer zu der damaligen Zeit vernetzt waren, eine beachtliche Menge, die dadurch generiert wurde, dass der Wurm auf mehreren verschiedenen Betriebssystemen laufen konnte. Der Morris Worm richtete keinen irreparablen Schaden an: Es wurden weder Dateien gelöscht noch die Funktionalität der Betriebssysteme verändert oder zerstört. Was allerdings passierte, war eine starke Verlangsamung der befallenen Maschinen, die den Wurm teilweise mehrfach ausführten, was schlussendlich den Arbeitsspeicher verstopfte und zu Abstürzen oder längeren Ausfällen der betroffenen Geräte führte (vgl. ebd., 446–447). Nach nur zwei Tagen wurde die Verbreitung des Wurms gemeinsam von den IT-Abteilungen der Universitäten Berkeley und Purdue gestoppt (vgl. ebd., 447). Spafford (ebd.) verliert ebenfalls einige Worte zur medialen Berichterstattung über den Wurm, und vermutet, dass Vertreter_innen der Presse den Morris Worm als Virus bezeichneten, »possibly because their experience to date has been only with that form of security problem.« Dies mag eine Erklärung für die Verwechselung sein – eine andere wäre, dass die Medialität des Wurms der von Computerviren in einem entschei-

34 Die folgende Geschichte ist doppelt so unterhaltsam, wenn man weiß, dass Robert Morris der Sohn des damals leitenden Wissenschaftlers des National Computer Security Center (NCSC) der National Security Agency (NSA) ist (vgl. Kocher 1989, 3).

denden Punkt – der Verbreitung über ein Netzwerk – ähnelt, was ausschlaggebend für diese Verwechselung oder bewusste Komplexitätsreduktion in der Berichterstattung war. Mit Ross lässt sich noch ein weiterer Grund ausmachen: Die Berichterstattung über den Morris Worm, so seine These, forcierte die Intersektion von Informatik und Medizin, da das Thema Computerviren leicht mit dem bereits etablierten und die Medien der damaligen Zeit dominierenden Diskurs über HIV/AIDS verknüpft werden konnte:

> »[M]edia commentary on the virus scare has run not so much tongue-in-cheek as hand-in-glove with the rhetoric of AIDS hysteria – for example, the common use of terms like killer virus and epidemic; the focus on highrisk personal contact (virus infection, for the most part, is spread through personal computers, not mainframes); the obsession with defense, security and immunity; and the climate of suspicion generated around communitarian acts of sharing.« (Ross 1991, 76)

Ross führt seine Überlegungen zum gemeinsamen Vokabular von HIV/AIDS und Computerviren anhand eines Artikels aus dem *Times Magazine* mit dem Titel *Invasion of the Data Snatchers* (vgl. Elmer-Dewitt 1988) weiter aus. Der Titel ist, wie Parikka (2016, 48) bemerkt, eine Anspielung auf Don Siegels Film INVASION OF THE BODY SNATCHERS (USA 1956), eine Adaption des zwei Jahre zuvor erschienenen Romans *The Body Snatchers* von Jack Finney. INVASION OF THE BODY SNATCHERS erzählt die leise, fast schon heimliche Invasion einer beschaulichen US-amerikanischen Kleinstadt in den 1950er Jahren durch Aliens, die die Bewohner_innen der Stadt durch identisch aussehende, sogenannte »pod people« austauschen, die keine Gefühle haben und daher der einzigen Eigenschaft beraubt sind, die sie menschlich gemacht hätte. Diese Geschichte kann als eine Parabel gelesen werden, in der Kommunismus und die Angst vor einer kommunistischen Infiltration der McCarthy-Ära anhand von Körperlichkeit und Un/Sichtbarkeit verhandelt werden (vgl. Ebert 1994).[35] Durch die Verwendung von Science Fiction-Motiven wie die Invasion, und in diesem Fall

35 Der Filmkritiker Roger Ebert schrieb über Abel Ferraras Remake des Films im Jahr 1994, das nur BODY SNATCHERS (USA 1993) heißt, dass, während jedem der insgesamt drei Verfilmungen des Stoffs eine unterschiedliche Motivation zu Grunde liege (von »the paranoia of McCarthyism« über einen Generationsunterschied), in diesem Fall »fear of AIDS« den Film informiert haben könne (Ebert 1994). Dies zeigt, dass das immunologisch strukturierte Narrativ des Stoffes in seiner konkreten Bedeutung historisch variabel und in seiner letztendlichen Ausgestaltung dem jeweiligen Zeitgeist unterworfen ist.

auch die Kolonisierung durch Außerirdische, verbindet der *Times*-Artikel, wie Ross (1991, 76) es formuliert, Computerviren mit »those historical fears about bodily invasion, individual and national, that are endemic to the paranoid style of American political culture.« Mit Parikka (2016, 48, Herv. MS) lässt sich darauf hinweisen, dass die Aliens, die unsichtbar und schwelend die US-amerikanische Kleinstadt unterwandern, als »threats to the idea of American *liberal freedom*« begriffen werden können, »and the allegory of viruses represented them as somewhat similar: they were threats to the basis of organized society, democracy, and civil rights.« Die liberale Vorstellung von Freiheit bildet, wie bereits mit Daniel Loick (2021, 267) ausgeführt wurde, die Grundlage für den negativen Sicherheitsbegriff, der den Staat in die Position der Kontrollinstanz der Einhaltung von Gesetzen, und damit der Aufrechterhaltung von Grenzen rückt. Zentraler Schauplatz dieses Grenzschutzes ist das Privateigentum (vgl. ebd., 270). Dies zeigt sich sowohl in der sich in den 1980er Jahren herausbildenden gesetzlichen Regulierung von Hacking als auch in den auf den Morris Worm folgenden Diskussionen über ethische Grundsätze der Computernutzung. 1986 wurde in den USA der *Computer Fraud and Abuse Act*, der die unautorisierte Computernutzung unter Strafe stellt, als Ergänzung des bestehenden Strafrechts zur Regulierung der Nutzung von Telekommunikationsmedien verabschiedet. Diese Entwicklung beschreibt Paul Taylor (2001, 115–118) als zusammenhängend mit der Professionalisierung der Computerbranche als Wirtschaftszweig, und der daraus erwachsenden Forderung nach dem Schutz ihrer wirtschaftlichen Interessen:

> »Hackers, along with viruses, can be portrayed as an external threat to security against which computer security professionals and their products are needed as a safeguard. At the same time, however, there also seems to be an implicit recognition that computer systems are inherently susceptible to bugs and intrusions but that some sort of social solution to such vulnerabilities is more realistic than finding the necessary technical resources to fix the problems.« (Ebd., 117)

Was die Herausbildung von ethischen Grundsätzen der Computernutzung innerhalb liberaler gesellschaftlicher Strukturen angeht, wurde Hacking vornehmlich mit Tropen und Metaphern der Grenzverletzung und -überschreitung belegt. Eine dieser Tropen, die sich bis heute gehalten hat, ist die des *Wilden Westen*s. Ein aktuelles Beispiel findet sich auf der Webseite des *No More Ransom Project*, einer Initiative der Sicherheitsfirmen *Kaspersky Lab* und *McAfee*, der niederländischen Polizei und *Europol*. Dort hilft ein »Crypto She-

riff« (vgl. The No More Ransom Project o.J.a), den eigenen Computer im Fall eines Ransomware-Befalls zu reparieren, indem die Ransomware identifiziert und, wenn möglich, eine Software zur Entschlüsselung der eigenen Daten angeboten wird. Der »Crypto Sheriff« kann als eine Anspielung auf das Bild von Hacker_innen als Cowboys betrachtet werden, das, wie Taylor (2001, 37–38) beschreibt, hauptsächlich auf William Gibsons 1984 erschienenen Science Fiction-Roman *Neuromancer* zurückzuführen ist. Das Wild West-Narrativ verbindet eine romantisierte Idee individualistischer Männlichkeit mit »frontier-based concepts« (ebd., 38), in denen *jungfräuliches* Territorium betreten wird und Grenzen verschoben oder verletzt werden (vgl. ebd., 37–38).[36] Weitere »frontier-based concepts« sind die des »breaking and entering«, also des Einbrechens, des Knackens, des Brechens, die es erlauben, Eigentumsrecht für immaterielle Güter zu denken und geltend zu machen (vgl. ebd., 145–151), sowie Metaphern aus dem Bereich der Körperlichkeit. Da der zentrale Schauplatz des Liberalismus die staatliche Regelung von Privateigentum ist, ist die Kriminalisierung von Hacking von elementarer Bedeutung, da der Staat nun auch die Grenzen immaterieller Güter schützen kann und muss.

Noch bevor Robert Morris die Autorschaft des Wurms bestätigte oder es ein entsprechendes Gerichtsurteil gab, das ihn eindeutig als Urheber desselben identifizierte, wurde der Nachweis über seine Autorschaft erbracht, da in seinen Useraccounts auf mehreren Computern der Cornell University ältere Versionen des Wurm-Codes gefunden wurden (vgl. Spafford 1989, 462). Was unklar blieb, und zu Spekulationen einlud, war Morris' Motivation. Während der Wurm von einigen als ein Dummer-Jungen-Streich abgetan wurde, war der Kanzler der Cornell University ganz vom Gegenteil überzeugt. Sein Bericht unterstellte Morris bösartige Absichten, und befand sein Verhalten für »unethical and contrary to the standards of the computer profession« (ebd., 463). Ross (1991, 85) konzentriert sich auf den Teil des Berichts, in dem Morris' bisherige Universitätslaufbahn besprochen wird: »[T]he report regrets that Morris was educated in an ›ambivalent atmosphere‹ where he ›received no clear guidance‹ about ethics from ›his peers or mentors‹ (he went to Harvard!).« In Kombination mit den gegen Morris erhobenen Anschuldigungen identifiziert

---

36 Taylor versammelt in *Hackers. Crime in the digital sublime* die Aussagen zahlreicher Hacker_innen, mit denen er E-Mail-Interviews geführt hat. Im Verlauf des Buches wird deutlich, dass die Wild West-Trope zwar von manchen affirmiert wird, aber auch starke Kritik an dieser und den anderen Tropen der Grenzaushandlung formuliert wird (vgl. Taylor 2001, 156–158).

Ross (ebd., 85–86) den Bericht als einen liberalen Abwehrmechanismus: Indem Morris vorgeworfen wird, *trotz* seiner liberalen Werten folgenden Erziehung keine ethischen Standards, kein klares Bewusstsein für Recht und Unrecht zu haben, wird Morris als schuldig, die Institution aber als schuldlos konfiguriert, ohne den Liberalismus selbst zu adressieren:

> »Generally speaking, the report affirms the genteel liberal ideal that professionals should not need laws, rules, procedural guidelines, or fixed guarantees of safe and responsible conduct. Apprentice professionals ought to have acquired a good conscience by osmosis from a liberal education, rather than from some specially prescribed course in ethics and technology.« (Ebd., 86)

Morris wurde für ein Jahr von der Universität suspendiert, und musste sich in Syracuse, New York vor Gericht verantworten (vgl. Ferbrache 1992, 23; Spafford 1989, 464). Die Anklage basierte auf dem *Computer Fraud and Abuse Act*, und Morris wurde im Frühling 1990 schuldig gesprochen und zu drei Jahren Bewährung, sowie 400 Sozialstunden und einer Geldstrafe von 10.000 US-Dollar verurteilt (vgl. Galloway 2004, 183).

3.4 AIDS und Computer

Der erste Computervirus, so erzählt es jedenfalls Fred Cohen, wurde im Gegensatz zu den bereits in Netzwerken heimischen Computerwürmern nicht ebenfalls dort beobachtet, sondern gewissermaßen unter Laborbedingungen hergestellt: Am 03.11.1983, schreibt Cohen (1987, 31), wurde er im Zuge eines Experiments konstruiert, das Teil eines wöchentlich stattfindenden Seminars über Computersicherheit war.[37] Die Durchführung des Virus-Experiments inklusive der getroffenen Sicherheitsmaßnahmen, mit denen eine unkontrollierte Vermehrung der neuen Software verhindert wurde, werden ausführlich beschrieben: Alle ›Infektionen‹ mussten von einer Person manuell bestätigt werden, und die Virussoftware war darüber hinaus so programmiert, dass sie keinen Schaden anrichten, sondern lediglich einen Nachweis über ihre Verbreitung erbringen sollte – nicht zuletzt auch, um eine unbemerkte Verbreitung zu verhindern (vgl. ebd.). Die erste Software, die in diesem Experiment

37 Spafford (1989, 449) hingegen weist darauf hin, dass bereits 1982 erste Computerviren im Umlauf waren.

mit dem Virus ausgestattet wurde, war ein Programm zur graphischen Darstellung des UNIX-Dateisystems mit dem Namen *vd*. Stefan Helmreich (2000, 476) folgend, zeigt sich an dieser Stelle zum ersten Mal ein »metaphorical link between computer viruses and sexually transmitted diseases« – Helmreich deutet *vd* in diesem Zusammenhang als die Abkürzung für *venereal disaease*, dem (mittlerweile veralteten) englischen Ausdruck für Geschlechtskrankheit. In den darauffolgenden Jahren sollte sich diese Verstrickung anhand von HIV/AIDS auf der Ebene der Imagination von Computern als Körpern, sowie der Herstellung von Sicherheit fortschreiben, und zwar sowohl im öffentlichen als auch im innerfachlichen Diskurs. Nennenswert für letzteren ist, wie Ross ausführt, dass die Verknüpfung von medizinischer Forschung und Informatik im Nachgang des Morris Worm aktiv von den Informatiker_innen hergestellt wurde, die den Computerwurm untersuchten und zu dem Schluss kamen, dass direkte Analogien zwischen den Verbreitungsmechanismen biologischer und elektronischer Viren (oder in diesem Fall: Würmer) bestünden, und basierend auf dieser Erkenntnis Sicherheitspläne entwarfen:

> »The epidemiology of biological virus (especially AIDS) research is being studied closely to help implement computer security plans. In these circles, the new witty discourse is laced with references to antigens, white bloodcells [sic!], vaccinations, metabolic free radicals, and the like.« (Ross 1991, 76)

Dies kann zweifelsohne als ein Effekt der medialen Gemeinsamkeiten von biologischen Viren und Computerwürmern, vor allem im Hinblick auf ihre Verbreitung in Netzwerken, gedeutet werden.[38] Als Reaktion auf den Morris Worm, führt Ross (ebd.) weiter aus, versuchten verschiedene Behörden der USA, ein »Center for Virus Control« einzurichten, das, wie er bemerkt, »Atlanta's Centers for Disease Control, notorious for its failures to respond adequately to the AIDS crisis« nachempfunden war. In der zweiten Hälfte der

38 Parikka (2016, 103) bemerkt, dass AIDS als eine »epidemic in non-scalar networks« betrachtet werden könne. Auch Albert-László Barabási (2002, 123–142) weist in *Linked. The New Science of Networks* darauf hin, dass sowohl HIV als auch Computerviren sich in skalenfreien Netzwerken verbreiten, was die ähnlichen Dynamiken der beiden bedinge. Seine sensationalistische Darstellung des Sexuallebens des homosexuellen Flugbegleiters Gaetan Dugas, anhand dessen Barabási seine Argumentation über die Verbreitung von HIV entfaltet, sowie seine moralistische Abwertung von Promiskuität zeugen jedoch von den in der Wissensproduktion über HIV tief verwurzelten homophoben Narrativen, die Barabási leider unreflektiert übernimmt.

1980er Jahre gelangten, abgesehen vom Morris Worm, auch einige Computerviren zu größerer Bekanntheit: der *Lehigh*[39] *Virus*, der *Jerusalem*[40] *Virus* und der *Cascade*[41] *Virus*. Diese neuen Computerviren wurden zunächst innerhalb der Fachöffentlichkeit mit AIDS verglichen: Der Lehigh Virus beispielsweise bekam den Beinamen »PC AIDS« (Parikka 2016, 113). Zum *Jerusalem Virus* zitiert Parikka (ebd., 112) aus *The Risk Digest*, einem Forum über IT-Sicherheit, das vom *ACM Committee on Computers and Public Policy* betrieben wurde, in dem es heißt: Der *Jerusalem Virus* »might do to computers what AIDS has done to sex. [...] The current free flow of information will stop. Everyone will be very careful who they come into contact with and with whom they share their information.« 1990 kursierten außerdem der *AIDS II*-Virus für das Betriebssystem MS-DOS, sowie *CyberAIDS* für Apple-Computer (vgl. McKinney/Mulvin 2019, 476–477).

Die bisherigen Ausführungen zum Zusammenhang von HIV, AIDS und Sicherheitsproblemen vernetzter Systeme haben sich hauptsächlich auf die Gemeinsamkeiten der Medialität dieser Phänomene, sowie die innerfachliche Perspektive der Informatik konzentriert. Mit der im letzten Unterkapitel umrissenen Herausbildung von ethischen Grundsätzen für die Nutzung von Computern, die an einem liberalen Freiheitsbegriff orientiert sind, sowie der Professionalisierung der Herstellung von Computersicherheit als Industriezweig Ende der 1980er/Anfang der 1990er Jahre und dem ungefähr zeitgleichen Einzug von PCs in Privathaushalte rückten zusätzlich User_innen als Adressat_innen der HIV/AIDS-Metaphorik in den Blick. »[N]ew and would-be computer users«, führen McKinney und Mulvin (ebd., 485) aus, »often confronted explanations of their vulnerability to technological systems through

39 Der *Lehigh Virus* (Betriebssystem: DOS) ist nach seiner Entdeckung im Jahr 1987 an der Lehigh University benannt. Dieser Virus zerstörte die COMMAND-Routine des DOS-Systems, die dafür zuständig ist, den Computer hochzufahren. Bemerkenswert an diesem Virus ist, dass er so schädlich war, dass er sich nicht effektiv außerhalb der Universität verbreiten konnte. Dennoch führte er zu der Einrichtung einer USENET-Gruppe über Computerviren (vgl. Parikka 2016, 33).

40 Der *Jerusalem Virus* (Betriebssystem: DOS) verfügte über eine eingebaute ›Zeitbombe‹: Am 13. Mai 1988, zum 40jährigen Bestehen des Staates Israel, sollte die Schadensroutine des Virus aktiviert werden, die darin bestand, alle aufgerufenen Dateien (und Software) zu löschen (vgl. danooct1 2012b; Parikka 2016, 81, Fußnote 147).

41 Der *Cascade Virus* (Betriebssystem: DOS) sorgte dafür, dass alle 30 Sekunden alle angezeigten Buchstaben auf einem Display alle nacheinander auf den Boden der Anzeige fallen (vgl. danooct1 2012a; Parikka 2016, 33–34).

the heuristics of HIV/AIDS […].« McKinney und Mulvin (ebd., 494) weisen zudem darauf hin, dass zu Beginn der 1990er Jahre die Bedeutung von Computernutzung und Vernetzung über das Internet einem gesellschaftlichen Aushandlungsprozess unterworfen war:

> »In the global North, the 1990s marked a period of heightened flexibility in the interpretation of what computing meant and would come to mean. With every new promise of what a networked computer could do came corresponding fears and threats. Analogies and metaphors were instrumental in simplifying and stabilizing the meaning of new technologies and the practices surrounding them. HIV/AIDS provided a ready template for interpreting the future of computing's domestication.«

Die scheinbare Selbstverständlichkeit dieser Metaphorisierung, und die ihr zugeschriebe Rolle der diskursiven Absicherung birgt jedoch, gemessen an der Geschichte von HIV und AIDS, ein verhältnismäßig großes Irritationspotential. In Aussagen wie »It might do to computers what AIDS has done to sex« (Parikka 2016, 112) scheint klar zu sein, was HIV/AIDS bedeutet, und scheint die Analogie dementsprechend eine klare Handlungsanweisung zu erzeugen: die Reduktion von Vernetzung. Nimmt man Treichlers Bestimmung von AIDS als *epidemic of signification* allerdings ernst, und rechnet man die Tatsache mit ein, dass die Versuche, zu bestimmen was AIDS sein könnte, von großen Unsicherheiten und anhaltenden gesellschaftlichen Aushandlungsprozessen gekennzeichnet waren (und es noch sind), so muss ein Prozess am Werk sein, der die Analogie von Computersicherheit und Schutz vor HIV/AIDS als eindeutig erscheinen lässt. Das vorliegende Unterkapitel wird diesen Prozess diskutieren, und darlegen, dass die Ambivalenzen des HIV/AIDS-Diskurses zugunsten einer liberalen Idee von Eigenverantwortung verflacht wurden, die sich in den homophoben Narrativen des HIV/AIDS-Diskurses zeigte, und die auf die Herstellung von IT-Sicherheit übertragen wurde. Dies wird im Folgenden anhand der Bedeutung des Immunsystems als Figur der Differenzgenerierung im Konzept der »Digital Immunology«, sowie der Begriffe »Digital Hygiene« und »Safe Hex« nachvollzogen.

3.4.1 Technische Lösungsansätze: *Computer Immunology*

Mit Computerviren, -würmern und der Imagination von Computern als Körpern gewann das Konzept der *Computer Immunology* an Popularität. Diese Anwendung immunologischer Konzepte auf Maschinen drückte sich zunächst in

der Vorstellung aus, Computer könnten gegen Schadsoftware *geimpft* und damit *immunisiert* werden, wie die sprechenden Namen der ersten Antivirenprogramme zeigen, die beispielsweise »Flu Shot +, ViruSafe, Vaccinate, Disk Defender, Certus, Viral Alarm, Antidote, Virus Buster, Gatekeeper, Ongard, and Interferon« (Ross 1991, 79) lauteten. Obgleich die Wirksamkeit dieser ersten Antivirenprogramme relativ begrenzt war, da es nicht lange dauerte, bis Hacker_innen neue Viren programmiert hatten, gegen die die Antivirenprogramme keinen Schutz bieten konnten (vgl. ebd.), hat sich die Idee von Antivirus-Software als Impfung lange gehalten. Ferbrache (1992, 45) führt sie genauer aus:

> »Vaccination provides an extremely powerful technique in biological systems, promoting the development of natural immunity using attenuated viral material. Within the computer environment fragments of viral material may also be used – in this case the signature recognition strings which the virus uses to prevent repeated replication. These fragments may safely be added to existing cells (computer programs) and will protect against the virus.«[42]

Ferbrache (ebd.) spekuliert weiterhin über die Möglichkeit von Antikörpern in Computersystemen: Diese Rolle könnte »specific disinfection software« zukommen, »which would recognise the infected program and destroy the virus.« Heutige Antivirenprogramme verfügen über eine Kombination dieser beiden Eigenschaften. Die von Ferbrache angestellten Vergleiche von biologischen und informatischen Viren betreffen noch die Punkte Isolation und Quarantäne, Latenz und Inkubation, Träger, Diagnose, Eintrittspunkte und Vektoren, auf die an dieser Stelle allerdings nicht eingegangen werden soll, da sie für die weitere Analyse nicht zielführend sind. Umso zentraler ist allerdings der letzte Punkt seiner Liste mit dem Titel »AIDS«:

---

42 Zeitgenössische Antivirenprogramme funktionieren effizienter als die von Ferbrache imaginierten: Anstatt jedes einzelne Programm durch einen Einschluss des zu bekämpfenden Materials zu ›immunisieren‹, scannen Antivirenprogramme in regelmäßigen Abständen die Festplatte eines Computers. Finden sie dabei ein Programm, dessen Signatur mit einer in ihrer Datenbank befindlichen Signatur übereinstimmt, melden sie dies dem_der User_in. Die in den letzten Jahren bekannt gewordene Schadsoftware EMOTET konnte genau diesen Vorgang umgehen, indem der Code der Malware sich immer wieder verändert hat, und so unter dem Radar der Antivirenprogramme blieb. In diesem Fall spricht man von einem *polymorphen Virus* (vgl. CISO 2018).

> »Finally, the organism's internal protective systems may recognise legitimate cell material (erroneous decisions resulting from a scan for a virus, or analysis of system activity logs) and may remove legitimate programs. Equally, the virus may alter the operation of the anti-virus software in such a manner as to cause the deletion or corruption of valid data or programs. This could be compared to the Acquired Immuno-Deficiency Syndrome (AIDS) in humans.« (Ebd., 46)

Ein mögliches Gefahrenszenario liegt für Ferbrache also darin, dass das Immunsystem des Computers, sprich: das Antivirenprogramm, durch einen Computervirus beschädigt werden, und infolgedessen nicht mehr genau zwischen legitimen und illegitimen Programmen unterscheiden könne. Dies würde zu einer weiteren Schädigung des Computers führen, ebenso wie zu einer Anfälligkeit für andere Viren, ähnlich wie dies nach einer HIV-Infektion bei Menschen geschähe. Diese Art der Metapher, konstatiert Helmreich (2000, 487), und auch ihre Ausweitung auf vernetze Computer, »make[s] sense only when biological organisms and computers are both envisioned as ›coded texts‹ pasted together with the glue of information.« Diese diskursive Herstellung einer Vergleichbarkeit, die suggeriert, dass Computer und Körper der gleichen Ordnung angehörten, wird in Diskussionen von Computerviren als *Artificial Life* fortgeführt, die jedoch für die folgende Untersuchung nicht von Interesse sind.[43] Stattdessen soll genauer auf die Figur des Immunsystems eingegangen werden.

Der Begriff *Immunität* ist seit einigen Jahrtausenden in Gebrauch und verbindet, wie der Wissenschaftshistoriker Johannes Türk (2014, 107) ausführt, »medizinisches Wissen um den Körper mit einem Wissen um dessen Interaktionen mit seiner Außenwelt […].« Immunität stammt vom lateinischen *immunitas*, das wiederum vom Wort *munus* abstammt, das Verpflichtung, öffentliches Amt oder Aufgabe bedeutet (vgl. ebd.). Nach römischem Recht waren immune Einzelpersonen oder Gruppen von den Aufgaben befreit, die zur Aufrechterhaltung der Gesellschaft notwendig waren, wie beispielsweise der Ausübung öffentlicher Ämter oder der Abgabe von Steuern (vgl. ebd., 108). Im mittelalterlichen Europa kam dem Begriff der Immunität eine neue Dimension zu: Immunität bedeutete nicht mehr nur eine Befreiung von gesellschaftlichen Aufgaben, sondern auch die Fähigkeit, eigene Gesetze sowie eine

43 Vergleiche dazu exemplarisch Spafford (1994), sowie Parikka (2016, 173–237).

eigene Gerichtsbarkeit einzusetzen, und vermittelte so zwischen den Interessen von Kirche und Adeligen (vgl. ebd., 110). In der Phase der Herausbildung von Nationalstaaten entstand schließlich das Konzept der diplomatischen Immunität, das die Grundlage des internationalen Rechts darstellt – wer in diplomatischer Mission unterwegs war, war im fremden Staat straffrei (vgl. ebd., 111). »Der Begriff der Immunität«, fasst Türk (ebd., 112, Herv. i.O.) zusammen, »bezieht sich daher hier zunächst auf den *Staats*organismus, bevor er eine Eigenschaft des biologischen Organismus bezeichnet.« Ende des 19. Jahrhunderts formiert sich schließlich die Immunologie als Wissenschaft, und überträgt den Begriff der Immunität metaphorisch auf das körperliche Phänomen der Resistenz (vgl. ebd.). All diesen Bedeutungszusammenhängen ist gemeinsam, dass Immunität sich als Ausnahme auf eine Norm bezieht (vgl. ebd., 107), also eine Differenz herstellt.

An diesem Punkt lässt sich mit Donna Haraways Aufsatz *The Biopolitics of Postmodern Bodies: Constitutions of Self in Immune System Discourse* anschließen, in dem sie das Immunsystem als ein Objekt des 20. Jahrhunderts sowie als »elaborate icon for principal systems of symbolic and material ›difference‹ in late capitalism« (Haraway 1991b, 204) bestimmt. Der Prozess der Differenzgenerierung ist notwendig für die Herstellung von Bedeutung – ohne Differenz gibt es keine Zeichen, keine Sprache, keine Positionen, und vor allem keine Subjekte. Haraway (ebd.) geht es spezifisch um die Subjektivierungsprozesse von »biomedical, biotechnical bodies and selves in post-modern scientific culture in the United States in the 1980s.« Ausgehend von Treichlers Bestimmung von AIDS als *epidemic of signification* nähert sich Haraway den Feldern und Versatzstücken, die über das Immunsystem als differenzgenerierende Figuration verbunden sind: HIV/AIDS, Krieg, Verkörperung, feministische Science Fiction-Literatur, medizinische Praktiken und viele weitere (auf die an dieser Stelle leider nicht eingegangen werden kann, da sie zu weit weg führen). Das Immunsystem fungiert in all diesen Kontexten Haraway (ebd.) zufolge als

> »a map drawn to guide recognition and misrecognition of self and other in the dialectics of Western biopolitics. That is, the immune system is a plan for meaningful action to construct and maintain the boundaries for what may count as self and other in the crucial realms of the normal and the pathological.«

Die Unterscheidung von, und damit die Grenzziehung zwischen *self* und *other* lässt sich somit als Grundfunktion immunologischer Logik begreifen, was diese an die Grenzaushandlungen des Liberalismus anschlussfähig macht.

Dies schlägt sich auch im IT-Sicherheitsdiskurs nieder: Auf die Spitze getrieben wurde die Idee eine *Computer Immunology* Ende der 1990er Jahre im gleichnamigen Paper von Stephanie Forrest, Steven Hofmeyr und Anil Somayaji. Die Autor_innen beginnen ihren Text mit einer rhetorischen Volte, in der nicht mehr die Informatik Bezug auf die Immunologie nimmt, sondern umgekehrt: »Natural immune systems protect animals from dangerous foreign pathogens, including bacteria, viruses, parasites, and toxins. Their role in the body is analogous to that of computer security systems in computing.« (Forrest et al. 1997, 88) Durch diese mechanistische Beschreibung des Lebens erscheinen Computer als belebt, und als derselben Ordnung angehörend wie Tiere, und damit auch Menschen. Bereits im nächsten Satz wird dieser Zusammenhang jedoch in einer Immunisierungsstrategie des Textes gegen Kritik teilweise aufgelöst: »Although there are many differences between living organisms and computers, the similarities are compelling and could point the way to improved computer security.« (Ebd.) Das von Ferbrache identifizierte und mit AIDS verglichene Problem der Sicherheitsmechanismen in Computern, Schadsoftware unter Umständen nicht korrekt erkennen zu können, sehen auch Forrest, Hofmeyr und Somayaji (ebd., 90) als grundlegend, und formulieren es in der bereits mit Haraway diskutierten Formel des Immunsystems, die in der Unterscheidung von *self* und *other* liegt: »The problem of protecting computer systems from malicious intrusions can similarly be viewed as the problem of distinguishing self from dangerous nonself.« Zeitgenössische, durch Software implementierte Sicherheitsmechanismen, wie beispielsweise Firewalls, so schreiben sie weiter, »have largely failed to take advantage of what is known about how natural biological systems protect themselves from infection.« (Ebd.) Für elaboriertere Sicherheitsmaßnahmen eines Computer-Immunsystems definieren Forrest, Hofmeyr und Somayaji (ebd., 91) sechs grundlegende Aufgaben, über die eine Software, der die Rolle des Immunsystems zukommt, verfügen solle:

> »[…] a stable definition of self, the ability to prevent or detect and subsequently eliminate dangerous foreign activities (infections), memory of previous infections, a method for recognizing new infections, autonomy in managing responses, and a method of protecting the immune system itself from attack […].«

Im Verlauf ihres Artikels stellen die drei Autor_innen einige Überlegungen zu der technischen Realisierung eines solchen Systems vor, die aber durchaus noch weiterer Entwicklung bedürfen. Dazu gehört unter anderem die Mit-

einbeziehung autorisierter User_innen in das *self* des Computers, die, so spekulieren sie, beispielsweise über »user behaviour patterns, or even keyboard typing patterns« (ebd., 91) erkannt werden könnten, obwohl diese Herangehensweise die Gefahr berge, ein zu restriktives System zu entwickeln. Der Artikel endet mit einer Evaluierung der Forschungsergebnisse, gemessen an den zeitgenössischen Möglichkeiten der IT-Sicherheit, in der die Autor_innen darauf hinweisen, dass der Erfolg oder Misserfolg von *Computer Immunology* darin begründet liege, den korrekten Abstraktionsgrad der Immunsystem-Analogie zu bestimmen (vgl. ebd., 96). Als ein kritisches Unterscheidungsmerkmal von Immunologie und auf Computer bezogener Sicherheit machen sie aus, »that the immune system is not concerned with the important problems of protecting secrets, privacy, or other issues of confidentiality.« (Ebd.) Dies deutet darauf hin, dass sie einen fundamentalen Unterschied zwischen kryptographischer Sicherheit und IT-Sicherheit sehen. Aber ließe sich nicht auch das Schützen von Geheimnissen mit immunologischen Analogien ausdrücken? Wird beispielsweise eine Nachricht verschlüsselt, um nur von einer bestimmten Person gelesen werden zu können, muss die Unterscheidung von *self* und *other* zuverlässig funktionieren, denn sonst wäre die Verschlüsselung nicht zu gebrauchen. Das Element des *störenden Dritten* ließe sich in diesem Fall als *other* bezeichnen, wobei *self* Sender_in und Empfänger_in, sowie deren Computer meint. Dies verkompliziert Forrest, Hofmeyr und Somayajis Modell, das nur die Definition von *self* innerhalb *eines* Computers (in Verbindung mit dem_der dazugehörigen User_in) in den Blick nimmt. Doch selbst wenn eine solche Erweiterung möglich wäre: Ganz so eindeutig geht es auch Ende der 1990er Jahre in der Kryptographie nicht mehr zu.

Exkurs: Kryptovirologie

Die vom *AIDS Information Trojaner* verwendete Verschlüsselung war, gemessen an heutigen Standards, recht schwach: Es wurde eine monoalphabetische Substitutionschiffre verwendet (vgl. Gazet 2010, 78), was bedeutet, dass, einmal dechiffriert, die Lösung auf jede weitere Installation der Malware anwendbar war. Und tatsächlich wurde die Verschlüsselung schnell gebrochen: Nachdem die Herausgeber_innen des Magazins *PC Business World*, an dessen Abonnent_innen der auf der AIDS Information Diskette 2.0 enthaltene Trojaner postalisch zugestellt wurde, von dem Missbrauch ihrer Adressliste erfuhren, engagierten sie einen Experten für Computerviren, um den Schaden wieder rückgängig zu machen. Dieser schrieb ein Programm mit dem Namen AIDSOUT, mit dem die Verschlüsselung des Trojaners wieder entschlüsselt werden

konnte (vgl. McKinney/Mulvin 2019, 484). Dies ist in zweifacher Hinsicht bemerkenswert: Einerseits, da der Trojaner durch die Angabe einer scheinbar einzigartigen Referenznummer (vgl. Solomon et al. o.J.) in der als Lizenzerneuerungsformular gestalteten Lösegeldforderung suggerierte, dass jeder betroffene Computer einzeln freigeschaltet werden müsse, und andererseits, da es deutlich werden lässt, wie prekär die AIDS-Analogie für Computer ist: Während es keine erfolgreichen[44] Therapiemöglichkeiten für HIV und AIDS[45] bei Menschen gab, war AIDS im Computer vollständig und nahezu instantan ›heilbar‹.[46] Dies sollte sich schon bald ändern: Nur sieben Jahre nach dem *AIDS Information Trojaner* erreichte die Grundidee der Ransomware ihre nächste Stufe, die gleichsam das technologische Bindeglied zwischen dem *AIDS Information Trojaner* und *WannaCry* darstellt. 1996 veröffentlichten Adam Young und Moti Yung ein Paper über eine Vermischung von Computerviren und kryptographischen Verfahren, die sie *Kryptovirologie* (englisch: *cryptovirology*) nannten. Die dazugehörige Angriffsvariante bezeichnen sie als »cryptoviral extortion attack« (Young/Yung 2017, 25). Dieses Phänomen ist heute unter dem Namen *Ransomware* bekannt (vgl. ebd.).

Kryptovirologie markiert seinen beiden Erfindern zufolge einen Shift im Feld der Kryptographie weg von dem Schutz vor Computerviren hin zum Angriff auf Daten (vgl. Young/Yung 1996, 129). In einem jüngeren Paper mit dem Titel *Cryptovirology: The Birth, Neglect, and Explosion of Ransomware*, das Young

44 Das Medikament Azidothymidine (AZT), das in den USA ab 1986 in klinischen Studien verabreicht wurde, wirkte zunächst vielversprechend, stellte sich aber im Verlauf der Studie als nur kurzzeitig wirksam, sowie von enormen Nebenwirkungen begleitet heraus, was zu heftigen Auseinandersetzungen zwischen Pharmaindustrie, Medizin und Aktivist_innen führte (vgl. Schock/Würdemann 2017; Treichler 1991).

45 (Präventive) Behandlungen der opportunistischen Infektionskrankheiten, wie etwa der Pneumocystis-Pneumonie, wurden allerdings bereits erfolgreich durchgeführt, und hatten auch verlangsamende Auswirkungen auf den Krankheitsverlauf insgesamt (vgl. Treichler 1991, 66–67).

46 Der *AIDS II*-Virus lässt sich als Spiel mit diesem Gegensatz deuten, da die Schadensroutine explizit auf die Un/Möglichkeit der Heilung Bezug nimmt. Dies geschieht in Form einer von schwarzen und weißen Smileys eingerahmten Nachricht: »I have been elected to inform you that throughout your process of collecting and executing files, you have accidentally ¶HÜ¢KΣ▶ yourself over; again, that's PHUCKED yourself over. No, it cannot be; YES, it CAN be, a √ìτûs [virus] has infected your system. Now what do you have to say about that? HAHAHAHAHA. Have ¶HÜÑ [phun] with this one and remember, there is NO cure for AIDS« (McKinney/Mulvin 2019, 477).

und Yung anlässlich der *WannaCry*-Welle verfassten, stärken sie diese Behauptung und weiten sie aus:

> »Cryptography, for millennia, had been perceived as a purely protective technology, and in particular as a way to hide the content of messages, secure data at rest, and authenticate users.« (Young/Yung 2017, 24)

Kryptovirologische Angriffe hingegen »weaponize cryptography as an attack tool as opposed to the previous uses that were defensive in nature.« (Ebd., 25) Dies mag zunächst verwundern, denn seit dem Zweiten Weltkrieg wurde Kryptographie in den USA rechtlich als eine Form von Munition eingestuft, also vorrangig als Militärtechnologie angesehen (vgl. Diffie/Landau 2007, 728). Diese Behauptung erklärt sich allerdings aus der Funktionsweise kryptovirologischer Angriffe. Über die ursprüngliche Zielsetzung ihres Forschungsvorhabens schreiben Young und Yung (1996, 131):

> »We are interested in making the host dependent on the virus. Thus, we design cryptovirology from the point of view of survivability. That is, a virus can survive in the host if it makes the host depend in a critical way on the very presence of the virus itself. If we cannot achieve this, we may approximate it by writing a virus such that its effect on the host is only reversible by the virus writer (so the dependence is approximated by making the host depend on the author rather than the virus).«

Letzteres ist ihnen durch die Kombination von asymmetrischer Kryptographie mit Computerviren[47] auch gelungen – der kryptovirologische »high survivability virus« (ebd., 130) zeichnet sich aus Sicht des Virus durch eine hohe Überlebensfähigkeit aus: Von dem Computer, den er infiziert hat, kann er nicht einfach entfernt werden. Als Inspiration für ihr Vorhaben nennen Young und Yung (ebd., 131) unter anderem den *AIDS Information Trojaner*, den sie trotz seiner leicht zu brechenden Verschlüsselung als einen ersten Schritt in die Richtung eines »high survivability virus« bezeichnen, aber auch den von H.R. Giger entworfenen *Facehugger*[48] aus Ridley Scotts Film ALIEN (UK/USA 1979).

---

47 Young und Yung (1996, 131) verwenden Virus als Überbegriff für Computerviren, Trojaner, Würmer und andere Sorten Malware.

48 Der *Facehugger* ist die erste Stufe des *Xenomorph*, also des titelgebenden Aliens, der, wenn er sich einmal an das Gesicht eines Menschen (oder Androiden) geheftet hat, um dessen Körper als Wirt für die nächste Stufe des *Xenomorph* zu gebrauchen, nicht mehr entfernt werden kann, ohne dabei den Wirt zu töten. Young and Yung (2017, 25) kommentieren: »We sought a digital analogue of the facehugger, namely, a forced

Ein bereits eingeführtes Beispiel für eine »cryptoviral extortion attack« ist die Ransomware *WannaCry*, die genau nach den von Young und Yung beschriebenen Kriterien funktioniert: Der_die Angreifer_in generiert ein asymmetrisches Schlüsselpaar, hinterlegt den öffentlichen Schlüssel in der Schadsoftware, und behält den privaten Schlüssel. Die Schadsoftware infiziert einen Computer und verschlüsselt dessen Dateien mit einem auf dem Computer hergestellten symmetrischen Schlüssel, der im Anschluss an diesen Vorgang mit dem öffentlichen Schlüssel des_der Angreifer_in asymmetrisch verschlüsselt wird.[49] Schlussendlich erscheint die Lösegeldforderung, die neben den Kontaktinformationen des_der Angreifer_in und einer Zahlungsanweisung auch den symmetrischen Schlüssel als Ciphertext beinhaltet, der ebenfalls zwecks Entschlüsselung mitgesendet werden muss (vgl. Young/Yung 2017, 25). Theoretisch sollte im Fall der Bezahlung des Lösegelds der symmetrische Schlüssel als Plaintext an die erpresste Person zurückgesendet werden, sodass diese wieder Zugang zu ihren Daten erhält (vgl. ebd.). Damit ist der Effekt des »high survivability virus« also nur durch den_die Angreifer_in rückgängig zu machen.[50] Immunologisch ausgedrückt wird es mit der Verbindung von Schadsoftware und asymmetrischer Kryptographie in der Kryptovirologie also möglich, durch Verschlüsselung das *self*, das bei Forrest, Hofmeyr und Somayaji aus User_in und Computer, oder in der Kryptographie aus Sender_in, Empfänger_in und deren Computern bestand, auf den_die Angreifer_in, dessen_deren Computer und den Computer der

symbiotic relationship between a computer virus and its host where removing the virus is more damaging than leaving it in place.«

49 Das hybride Verfahren wird verwendet, da symmetrische Verschlüsselung schneller und weniger ressourcenaufwändig als asymmetrische Verschlüsselung ist. Ein ausreichend langer symmetrischer Schlüssel kann nicht in Polynomialzeit gebrochen werden, wie bereits in Kapitel 2 dargelegt wurde. Darüber hinaus muss bei diesem hybriden Verfahren nur der asymmetrisch verschlüsselte symmetrische Schlüssel an den_die Angreifer_in versendet werden, um eine mögliche Entschlüsselung zu gewährleisten, und nicht die gesamten verschlüsselten Daten der Festplatte.

50 Obwohl dieses Verfahren bereits seit 1996 bekannt ist, dauerte es noch ca. 20 Jahre, bis kryptovirologische Angriffe in großem Maß durchgeführt wurden, da Angreifer_innen Gefahr liefen, durch den Empfang des Lösegelds ins Visier der Strafverfolgungsbehörden zu geraten. Pseudonyme Kryptowährungen wie Bitcoin oder Ethereum lösten dieses Problem, und verwandelten Ransomware in ein regelrechtes Geschäftsmodell mit einem geschätzten Jahresumsatz von einer Milliarde US-Dollar (vgl. Young/Yung 2017, 25).

erpressten Person[51] zu beschränken, wodurch letztere zum *störenden Dritten* gemacht wird.

3.4.2 User_innenzentrierte Lösungsansätze: *Digital Hygiene/Safe Hex*

Mit dem *Digital Immunology*-Konzept wurde ein informatischer Ansatz vorgestellt, der die Herstellung von IT-Sicherheit in erster Linie softwarebasiert zu erreichen versucht: User_innen tauchen bei Forrest, Hofmeyr und Somayaji nur indirekt auf, nämlich in Form ihrer Effekte auf die Maschine, die, sofern sie von autorisierten User_innen kommen, irgendwie als dem *self* der Maschine zugehörig markiert werden müssen. Anhand der Funktionsweise von Kryptovirologie wurde eine Spielart von Schadsoftware vorgestellt, die die Relation von autorisierten User_innen und ihren Computern unterläuft und stört, indem erstere als das *störende Dritte* markiert und ausgeschlossen werden. Darüber hinaus wurde die Rolle von User_innen im vorliegenden Kapitel bisher nicht weiter bestimmt, was aber an dieser Stelle anhand der Konzepte *Digital Hygiene* und *Safe Hex* nachgeholt werden soll. Sowohl *Digital Hygiene* als auch *Safe Hex* zielen auf eine Regulierung des Verhaltens der Computernutzer_innen ab, die für die Herstellung von IT-Sicherheit mit verantwortlich gemacht werden.

Digital Hygiene

»The notions of digital hygiene«, schreibt Parikka (2016, 2), »orderly computing, and clean communication has [sic!] appeared in the vocabulary of computer culture since the 1980s.« Dies führt er auf das mit dem technologischen Fortschritt ab den 1980er Jahren einhergehende Körperideal zurück: »The clean body of modernization found its imaginary ideal in the computer organism.« (Ebd., 119) Verknüpft mit den Bildern digitaler Hygiene, ordentlicher Computernutzung und sauberer Kommunikation ist also das Konzept des Computers als maschinischem, sauber-elektronischem Körper. Helmreich (2000, 477) verbindet dieses Körperideal darüber hinaus mit dem Liberalismus der US-amerikanischen Gesellschaft, und konstatiert:

> »Computers are imagined as pristine, autonomous entities that exist prior to their embedding in networks – an idea that echoes the liberal conception

51 Der_die Angreifer_in hat zwar keinen Zugriff auf die Daten der erpressten Person, greift aber in ausreichendem Maß in die Funktionsweise von deren_dessen Computer ein, um Teil dieser Trias zu sein.

> of society as made up of individuals who exist prior to the society of which they are a part, an ideology deeply written into U.S. political culture.«

Doch der Körper des Computers blieb, wie in diesem Kapitel deutlich geworden ist, nicht lange diesem Ideal treu: »Just as the body biologic (and politic) was, from the end of the nineteenth century, the object of constant attacks by minuscule viruses and bacteria, so the computer soon had its own share of dirt.« (Parikka 2016, 119) Eine besonders bemerkenswerte Reaktion auf den ›Dreck‹ und die damit einhergehenden ›Krankheiten‹ der sauberen Systeme ist die Forderung nach *Public Health* für die vernetzte Gesellschaft (vgl. ebd.). Public Health lässt sich als »die Wissenschaft und die Praxis der Verhinderung von Krankheiten, Verlängerung des Lebens und Förderung der Gesundheit durch organisierte Anstrengungen der Gesellschaft« (Robert Koch-Institut 2016) definieren, und wird damit als eine biopolitische Maßnahme erkennbar. In ihrer Analyse von Foucaults Konzeptionen von Sicherheitsdispositiv und Biopolitik konstatiert Maria Muhle (2008, 261, Herv. i.O.) unter Bezugnahme auf Georges Canguilhems Begriff des Lebens: »Die Bio-Macht bezieht sich nicht nur *auf das Leben*, sondern sie tut dies zugleich *nach dem Modell des Lebens*.« Dies bedeutet konkret, dass die Bio-Macht das Leben reguliert, nicht indem sie es diszipliniert, oder gezielt auf einen Aspekt des Lebens wirkt, sondern indem sie sich multifaktoriell aufstellt, und über das Milieu die Bedingungen für das Leben reguliert. »Ein solchermaßen regularisierbares und indirekt erfassbares Leben«, so schreibt Muhle (ebd., 263) weiter, »verweist auf die spezifisch organische Dimension eines Lebensbegriffs, so wie ihn auch die moderne Biologie kennt.« Die vermutlich prominenteste Forderung innerhalb der Informatik für diese Form der Herstellung von Sicherheit, die sich an dem Wissen der modernen Biologie, vor allem der Immunologie orientiert, sowie über das Milieu die Bedingungen für sichere Informationstechnologie regulieren möchte, stammt von Bryan Kocher, der Ende der 1980er Jahre Präsident der *Association for Computing Machinery* (ACM) war. In seinem kurzen, aber viel zitierten Text mit dem Titel *A Hygiene Lesson*, den Kocher (1989, 3) als Einleitung zur offiziellen Publikation der ACM verfasst hat, reagiert er direkt auf den *Morris Worm*, den er als einen Streich, aber auch als Warnsignal begreift: Habe der Morris Worm zwar keinen Schaden angerichtet, so sei durch ihn doch unmissverständlich klar geworden, wie verletzlich vernetzte Systeme seien. Bemerkenswert ist, dass auch Kocher (ebd.) den Morris Worm als Virus bezeichnet, und zunächst Parallelen zu HIV/AIDS zieht: »The parallels between contracting a PC ›virus‹ and a sexually transmitted disease are

painfully obvious«, nur um wenig Sätze später die »UNIX epidemic«, also den Morris Worm, mit der Cholera-Epidemie des 19. Jahrhunderts gleichzusetzen. IT-Sicherheit, also *Security*, wird bei Kocher (ebd., 3–6) damit gleichbedeutend mit Hygiene, und somit Prävention:

> »Just as in human society, hygiene is critical to preventing the spread of disease in computer systems. Preventing disease requires setting and maintaining high standards of sanitation throughout society, from simple personal precautions (like washing your hands or not letting anyone know your password), to large investments (like water and sewage treatment plants or reliably tested and certified secure systems).«

Auf die Herkunft der hier von Kocher aufgerufenen Hygienemaßnahmen zur Prävention von Krankheiten, wie beispielsweise das Händewaschen oder die Einrichtung einer geregelten Frisch- und Abwasserversorgung innerhalb von Städten, geht auch Michel Foucault in seiner von 1977–1978 am Collège de France gehaltenen Vorlesung *Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I* ein, in der er die Bio-Macht untersucht. Bereits im ersten Teil zeichnet er die Entstehung des Sicherheitsdispositivs nach, und grenzt dieses von juristischen, juridischen und Disziplinarmechanismen ab. Während letztere durch Überwachungs- und Korrekturmechanismen gekennzeichnet sind, etabliert das Sicherheitsdispositiv statt einer binären Aufteilung in erlaubte und verbotene Ereignisse einen »als optimal angesehene[n] Mittelwert« (Foucault 2006, 20) für das Vorkommen bestimmter Ereignisse, sowie »Grenzen des Akzeptablen« (ebd.), jenseits derer ein bestimmtes Ereignis nicht mehr geschehen dürfe. Sicherheit ist also befasst mit der statistischen Verteilung von Elementen und Ereignissen. Daher arbeitet sie mit den materiellen Gegebenheiten eines Territoriums: »mit der Lage, dem Ableiten von Abwässern, mit den Inseln, mit dem Freiland usw. Sie bearbeitet folglich ein Gegebenes.« (Ebd., 38) Im Fall von Computersicherheit wären die materiellen Gegebenheiten sowohl die Hard- als auch die Software und die Vernetzung der Computer untereinander – oder für Kocher (1989, 6) »reliably tested and certified secure systems«. Ein entscheidendes Merkmal des Sicherheitsdispositivs ist allerdings, dass Sicherheit nicht als perfekt, nicht als absolut gedacht wird. Stattdessen

> »[…] geht [es] einfach darum, die positiven Elemente zu maximieren, so daß man auf bestmögliche Weise vorankommt, und im Gegensatz dazu Risiko und Mißstand, wie den Diebstahl, die Krankheiten usw., auf ein Mindestmaß zu beschränken, wobei man genau weiß, daß man sie niemals besei-

> tigen wird. […] Das wird nie aufzuheben sein, also bearbeitet man Wahrscheinlichkeiten.« (Foucault 2006, 38)

Auch Kochers Forderung bewegt sich in eine ähnliche Richtung. Es geht ihm weniger um absolute Sicherheit, als um eine andauernde Arbeit an ihrer Herstellung, was erkennen lässt, dass absolute Sicherheit nie ganz erreicht werden kann. Er bemerkt, dass nicht vernetzte Computer, ähnlich wie Einsiedler, die außerhalb von gesellschaftlichen Zusammenhängen stehen, so gut wie nie erkranken würden, für eine vernetzte Gesellschaft aber andere Regeln gelten müssten:

> »[…] if we are to become a networked society, we must treat computer diseases as a real threat to that society. We must heed the public health warnings from NSA, practice personal systems hygiene, adhere to sanitary standards, and support the development of secure systems to keep the germs out. Electronic epidemics should be like cholera epidemics – something you only read about in history books.« (Kocher 1989, 3–6)

Kochers Vision folgend, sollte die NSA eine ähnliche Rolle übernehmen wie die Centers for Disease Control und regelmäßige Gesundheitswarnungen aussprechen (der Versuch der Einrichtung eines den CDC ähnlichen Center for Virus Control als Reaktion auf den Morris Worm wurde bereits mit Ross (1991, 75–76) erwähnt), und müssten die Nutzer_innen vernetzter Computer keine neuen Techniken der Problemlösung erlernen, sondern könnten sich an dem gesellschaftlich vorhandenen Alltagswissen um die eigene Körperhygiene orientieren, das sie eigenverantwortlich auf ihre Maschinen anwenden sollen. Das Programm von »personal systems hygiene« bedeutet also, die eigene Körperhygiene auf die eigene Maschine auszudehnen, und so beide Körper als *self* vor allen biologischen und informatischen Formen von *other* zu schützen. Computer werden so nicht nur als Körper gedacht, sondern dem eigenen Körper gleichgestellt – eine Annäherung, die im Folgenden noch wichtig sein wird. Die Forderung nach einer Computerhygiene beinhaltet »a range of practices, demands, advice, and precautions« (Parikka 2016, 129), die bei Kocher von der Geheimhaltung von Passwörtern bis hin zu regelmäßigen Sicherheitszertifizierungen von IT-Systemen reicht. Auf diese Weise werden nicht nur Institutionen in die Pflicht genommen, für Sicherheit zu sorgen, sondern auch, wie Parikka (ebd.) schreibt, »the user and her way of interacting with the computer«, die zum »safe link in the networking chain«

werden sollen. Kochers Wunsch, über ›elektronische Epidemien‹ nur noch in Geschichtsbüchern zu lesen, hat sich dennoch nicht realisiert.

Safe Hex

Die zweite Ebene, auf der User_innen als für IT-Sicherheit Verantwortliche adressiert werden, ist eng mit der Idee von »personal systems hygiene« verbunden, rückt aber HIV und AIDS, die bei Kocher eine eher untergeordnete Rolle spielen, als Metaphern für schädliche Phänomene in vernetzten Computern ins Zentrum. Mit der metaphorischen Übertragung von AIDS auf Computerviren gehen nicht nur die medialen Gemeinsamkeiten der Übertragung durch Ansteckung einher, denn, wie Deborah Lupton (1994, 560) in ihrem Artikel *Panic computing: The viral metaphor and computer technology* konstatiert, »[v]iewing computer malfunction as a viral illness unavoidably invokes a moral framework.« Basierend auf Susan Sontags Untersuchung *Illness as Metaphor and AIDS and Its Metaphors* beobachtet Lupton (ebd., 561) in Bezug auf HIV und AIDS, dass der öffentliche Diskurs vor allem von Fragen nach Moral, Verantwortung und Schuld geprägt sei, wobei die letzten beiden stets den Kranken selbst zugewiesen werden.[52] Lupton (ebd., 561) schreibt weiter:

> »Public health discourse now emphasizes the responsibility of the individual to stay healthy, avoid risk and resist indulgence in certain behaviours defined as ›dangerous‹. It is believed that one does not become ill merely out of bad luck; one becomes ill because one has courted illness in some way, whether it be going out in the rain without an umbrella, eating too few vegetables and too much fat, suppressing anger in an inappropriate manner, or engaging in socially proscribed sexual acts.«

Für den HIV/AIDS-Diskurs der 1980er Jahre ist vor allem das Partizipieren in »socially proscribed sexual acts«, also verbotenen und verpönten Sexualpraktiken, von Bedeutung, das mit einer »homophobic representation of homosexuality« (Bersani 1987, 209) verknüpft ist. Bereits zu Beginn dieses Kapitels wurde mit Deuber-Mankowsky (2017b, 16) angerissen, dass in der AIDS-

52 Ein Beispiel für diese Moralisierung, die eine Infektion mit HIV als eigenes Verschulden formuliert, und gleichzeitig in einer zynischen Geste die Kontrollierbarkeit der eigenen Krankheit verspricht, ist die *New Age*-Bewegung und deren wohl prominenteste Vertreterin Louise Hay. »Die Ursache der Krankheit [AIDS, MS], so Hays Botschaft, ist Selbsthass, sie kann, so ihr Versprechen, geheilt werden durch Selbstliebe und Vergebung.« (Deuber-Mankowsky 2017b, 41)

Krise durch die konservative US-amerikanische Politik die »Krankheit […] zu einer Strafe und Homosexualität zu einer Sünde erklärt« wurde. Leo Bersani (1987, 210) analysiert die mit dieser Zuschreibung einhergehende diskursive Verschiebung: Schwule Männer seien nicht nur selbst schuld, wenn sie sich durch ihr Sexualverhalten mit HIV infiziert haben, mehr noch: »It is as if gay men's ›guilt‹ were the real agent of infection.« Aber worin genau, fragt sich Bersani weiter, besteht diese bereits vor einer HIV-Infektion da gewesene Schuld eigentlich? Bezugnehmend auf Simon Watney und weitere, von ihm nicht genannte Theoretiker_innen, bemerkt Bersani (ebd.), »[e]veryone agrees that the crime is sexual, and […] define[s] it as the imagined or real promiscuity for which gay men are so famous.« Sich dieser phantasmatisch-homophoben Verknüpfung weiter nähernd, kommt Bersani (ebd.) zu dem Schluss, »the act […] may itself be associated with insatiable desire, with unstoppable sex.« Dabei weisen die Vorstellungen von Mediziner_innen, die in der medialen Berichterstattung zu sehen und hören sind, wie Bersani (ebd., 211) mit Watney analysiert, Anklänge an die Diskursivierung weiblicher Prostituierter auf, die als Behältnisse für Geschlechtskrankheiten (konkret: Syphilis) imaginiert wurden, die sie angeblich an ›unschuldige Männer‹ weitergaben. Bersani (ebd.) schreibt weiter:

> »[T]he similarities between representations of female prostitutes and male homosexuals should help us to specify the exact form of sexual behavior being targeted, in representations of AIDS, as the criminal, fatal, and irresistibly repeated act. This is of course anal sex […].«

Konkret handelt es sich also um penetrativen Analsex, der, verschränkt mit der tatsächlichen und imaginierten Promiskuität homosexueller Männer zum Problem erklärt wird. Gerade die Vorstellung von homosexueller Promiskuität, von »gay men having sex twenty to thirty times a night, or once a minute«, führt Bersani (ebd.) aus, sei weniger mit den Fantasien männlicher als mit denen weiblicher Promiskuität belegt, die wiederum mit einer »fantasy of female sexuality as intrinsically diseased« zusammenhingen. Auf diese Weise werde Promiskuität nicht als das Infektionsrisiko erhöhend diskursiviert, sondern direkt zum »*sign of infection*« (ebd., Herv. i.O.). Die damit einhergehende Stigmatisierung von Promiskuität drückte sich auch in den am heteronormativen Ideal der *weißen* Kleinfamilie ausgerichteten Gesundheitsempfehlungen aus, die die Medienlandschaft dominierten (vgl. ebd., 203). So wurden unter anderem Monogamie und Abstinenz als wirksamer Schutz vor einer HIV-Infektion diskutiert, und *safe partners* sicheren

Sexpraktiken, also *Safe/r Sex*,[53] vorgezogen (vgl. Crimp 1987a, 252–253). Diese Empfehlungen sind, wie Douglas Crimp (ebd., 253) spitz bemerkt, an dem Mythos orientiert, »that monogamous relationships are not only the norm but ultimately everyone's deepest desire« – und darüber hinaus schützen sie, wie auch Bersani (1987, 218) schreibt, nicht zuverlässig vor einer HIV-Infektion. Doch in den Empfehlungen von Monogamie oder gar Abstinenz lässt sich nicht nur das heteronormative Familienideal erkennen, sondern auch der Versuch, HIV über eine Einschränkung der Verbreitungswege einzudämmen, nur mit, wie sich gezeigt hat, den absolut falschen Mitteln. Die Stigmatisierung ganzer Personengruppen als scheinbar einzigen Gefahrenherden für die Übertragung von HIV, und die Einschränkungen der körperlichen Verbindungen, die diese mit anderen eingehen könnten, statt der Sicherung dieser Verbindungen, hat sich als falsch und gefährlich erwiesen, »because people do not abstain from sex, and if you only tell them ›just say no‹, they will have unsafe sex.« (Crimp 1987a, 252–253)

Eine ähnliche Dynamik zeigt sich auch im IT-Sicherheitsdiskurs der 1980er und 1990er Jahre in den Versuchen der Regulierung körperlicher Verbindungen zwischen Computern: Auf die Unvereinbarkeit von Sicherheit vor viraler Software in vernetzten Systemen mit denselben hatte bereits Cohen (1987, 34) in *Computer Viruses. Theory and Experiments* hingewiesen. Dennoch ist ihm klar, dass Vernetzung nur durch Informationsaustausch realisiert werden kann, was also eine Koexistenz viraler Elemente und sicherer Computernetze unter »significant constraints« (ebd., 35) voraussetzt. Diese Einschränkungen werden durch die HIV/AIDS-Metaphorik auf die Nutzer_innen ausgelagert, die als Verantwortliche für die Sicherheit ihrer eigenen Computer, und vermittelt darüber auch der anderen Computer eines Netzwerks positioniert werden. »Where AIDS had created a new culture of bodily anxiety and political paranoia«, schreibt Parikka (2016, 34), »computer sex diseases were thought to create similar fears about communication and digital contact.« Ähnlich wie der medial dominante HIV/AIDS-Diskurs konzentrierte sich auch der IT-Sicherheitsdiskurs auf die Prävention von Ansteckungen, und die mediale

---

53 Die Bezeichnung *Safe Sex* entstand in den 1980er Jahren (vgl. Crimp 1987a). Heute hat sich in manchen Kontexten die Bezeichnung *Safer Sex* durchgesetzt, um zu betonen, dass es auch mit dem Einsatz von adäquaten Verhütungsmitteln keinen restlos sicheren Sex gibt – nur *sichereren Sex*. Die von den Aktivist_innen intendierte Bedeutung des Konzepts wird dadurch nicht verändert.

Berichterstattung über Computersicherheit, Werbematerialien für Antivirensoftware, Computerfachzeitschriften sowie Ratgeberliteratur zeichneten das Bild des unschuldig-reinen Computers, dessen Gesundheit in den Händen von sich potenziell gefährlich verhaltenden Nutzer_innen liege (vgl. ebd., 132–133). So formierte sich »the idea of a responsible user, who practiced digital hygiene and *safe hex*« (ebd., 179). *Safe Hex* ist jedoch im Gegensatz zu *Safe/r Sex* nicht mit der Entstigmatisierung von Promiskuität/hoher Konnektivität verbunden, sondern beinhaltet in erster Linie Verbots- und Verzichtsratschläge. Damit folgt *Safe Hex* weiterhin der Maxime der Eigenverantwortung der Nutzer_innen, die, falls sie dieser Verantwortung nicht gerecht werden sollten, eventuelle Schäden selbst verschuldet haben. Vor diesem Hintergrund lohnt sich ein erneuter Blick auf Brigitte Weingarts (2002, 80) Beschreibung der »Verwicklung der Ansteckungsgefahren« beim *AIDS Information Trojaner*:

> »Wer jede x-beliebige Diskette nicht als per se mit Vorsicht zu behandelnden ›Fremdkörper‹ erachtet, sondern in den ›intimen Öffnungen‹ seines Computers zuläßt, ist beim ersten Test – auf ›gesundes Mißtrauen‹ – schon durchgefallen. Er/sie hat sich mit dieser Fahrlässigkeit gewissermaßen schon in die ›Risikogruppe‹ katapultiert.«

Was Weingart hier als Subtext des *AIDS Information Trojaners* beschreibt, illustriert nicht nur die mit den HIV/AIDS-Metaphern einhergehende Verwicklung der Ansteckungsverfahren, sondern auch die Verwicklung der dominanten gesellschaftlichen Reaktionen, sowie die dem IT-Sicherheitsdiskurs eingeschriebene Homophobie: Haben die Nutzer_innen kein *Safe Hex* praktiziert, und ihren Computer ungeschütztem Verkehr mit einer fremden Diskette ausgesetzt, so sind sie auch selbst schuld an dem entstandenen Schaden. Als sichere Computernutzungspraktiken werden allerdings weniger Strategien für einen sicheren Umgang mit fremden Disketten oder (raub-)kopierter Software angeführt, als vielmehr der Appell, auf diese besser zu verzichten:

> »›Do not copy programs,‹ ›do not bring program disks from home to work,‹ ›do not boot your computer from an unknown disk,‹ ›check all disks before using them,‹ ›check all downloaded software before using it‹ – these and a range of similar recommendations were used to guide the user to proper PC habits.« (Parikka 2016, 136)

Die meisten dieser Ratschläge lassen sich mit Crimp als Verbote im Sinne einer unrealistischen »just say no«-Abstinenz begreifen, wohingegen wenigstens der Ratschlag, heruntergeladene Software vor dem ersten Ausführen zu

überprüfen, der Idee von *Safe/r Sex* so nahekommt, wie dies in Bezug auf Computer möglich ist. Gekoppelt mit den Verboten bei gleichzeitiger Forderung nach sicheren Computernutzungspraktiken war die Etablierung des Softwaremarkts. Sicherheitsprobleme wie Computerviren und -würmer werden damit, wie Parikka (ebd., 137) ausführt, verwendet um zwischen »healthy capitalist consumer products and software programs distributed as shareware or even freeware« zu unterschieden, sowie letztere als potenziell gefährlich zu markieren. Die bereits diskutierte Kriminalisierung von Hacking stellt einen weiteren Schritt in diese Richtung dar. Parikka (ebd.) schreibt weiter: »[C]leanliness and hygiene are what the consumer pays for. Trust has a cost. This demonstrates how consumer products succeed in their role as ›anxiety relievers.‹« Oder, wie sich mit Andrew Ross (1991, 76) polemisch hinzufügen lässt: »The underlying moral imperative is this: you can't trust your best friend's software any more than you can trust his or her bodily fluids. Safe software or no software at all!« Vertrauen ist also nur in kapitalistischen Strukturen denkbar, und so lässt sich *Safe Hex* bestenfalls als eine Schwundstufe des Konzepts von *Safe/r Sex* begreifen: In den meisten Fällen meint *Safe Hex* entweder Verzicht oder *Safe Partners*, wie beispielsweise vertrauenswürdige Softwarefirmen. Mit McKinney und Mulvin (2019, 487–488) lässt sich resümieren: »[I]n the 1990s, self-regulation and personal responsibility governed both mainstream public pedagogies around HIV and user responsibility in computing (and continue to do so today).«

Negative Sicherheit

> »The only computer that's completely secure […] is a computer that no one can use.« (Kaplan 2016)

Das vorliegende Kapitel hat bisher sowohl einen Blick auf die Anfänge von Schadsoftware geworfen als auch auf zeitgenössische Phänomene, um mit diesen in einer Kreuzstichbewegung Überlegungen zum Diskurs der IT-Sicherheit vorzustellen. Innerhalb dieses Spannungsfelds wurde sowohl grundlegendes Wissen der Informatik zur Beschaffenheit von Computerviren, -würmern und Kryptovirologie/Ransomware vermittelt, als auch medienwissenschaftliche Überlegungen zur Medialität derselben entwickelt. Darüber hinaus wurde die Verbindung des IT-Sicherheitsdiskurses mit dem AIDS-Diskurs der 1980er Jahre nachgezeichnet. Als kurzes Resümee lässt sich an dieser Stelle festhalten, dass die Herstellung von Sicherheit in IT-Systemen, die hier als vernetzte Computer gefasst wurden, immunologisch strukturiert

ist, insofern sie beständig mit Grenzaushandlungen beschäftigt ist. Donna Haraway folgend, die das Immunsystem als diskursive Figuration des 20. Jahrhunderts für die Differenzgenerierung, und damit die Unterscheidung von *self* und *other* analysiert hat, wurden die Grenzaushandlungen der IT-Sicherheit anhand der ersten Antivirenprogramme, aber insbesondere anhand des Konzepts der *Computer Immunology* von Stephanie Forrest, Steven Hofmeyr und Anil Somayaji sichtbar, bei dem ein computereigenes Immunsystem in Form von Software realisiert werden sollte. *Computer Immunology* markiert Schadsoftware als das *störende Dritte*, das aus den rechnerischen Prozessen von Computern ausgeschlossen und an seiner Verbreitung gehindert werden muss. Eine solche Herangehensweise, die die Herstellung von Sicherheit primär auf Software auslagert, musste notwendiger Weise scheitern, da die Unterscheidung erwünschter und unerwünschter Prozesse in vielen Fällen nicht eindeutig bestimmt werden kann. Dies liegt einerseits darin begründet, dass, wie mit Sybille Krämer aufgezeigt wurde, die Medialität von Computerviren und -würmern sich stark ähnelt, was hauptsächlich auf den beiden Phänomenen eigenen Prozess der Übertragung durch Ansteckung zurückzuführen ist. So werden diese Phänomene vergleich-, und mitunter verwechselbar, auch wenn sie aus informatischer Perspektive unterschiedlich definiert werden (vgl. Spafford 1989). Zusammengenommen mit Jussi Parikkas Feststellung, dass Schadsoftware als Bestandteil vernetzter digitaler Systeme begriffen werden müsse und nicht als ein ihnen äußerlicher Störfaktor, wird klar, dass das Immunsystem als strukturierende Metapher der IT-Sicherheit, was die Abwendung von Schaden angeht, in seiner Effektivität begrenzt ist: Aufgrund der Ambiguität viraler Prozesse, die sich sowohl in Schadsoftware als auch in erwünschter Software beobachten lassen, hat sich eine rein softwarebasierte Lösung für die Sicherheitsprobleme vernetzter Systeme als unzureichende Schutzmaßnahme herausgestellt. Mit den Konzepten der *Personal Systems Hygiene* und der HIV/AIDS-Metaphorik von *Safe Hex* wurde die Funktionsweise des Immunsystems auf die Nutzer_innen ausgedehnt, die so verantwortlich für die Gesundheit ihrer Computer wurden. Die immunologische Verfasstheit des IT-Sicherheitsdiskurses entfaltet auf diese Weise über die Verbindung von vernetzten Computern und HIV/AIDS eine normalisierende Wirkung, die bestimmte Formen der Computernutzung als normal und andere als nicht normal diskursiviert. Nahezu all diese Strategien und Praktiken basieren auf Grenzschutz, Exklusion und Abschottung, die kennzeichnend sind für den negativen Sicherheitsbegriff des Liberalismus (vgl. Loick 2021, 268–272). Dieser liegt damit, wie gezeigt werden konnte, nicht nur der Kryptologie,

sondern auch der IT-Sicherheit zugrunde. Das Wettrennen von Hacks und Sicherheitsupdates, wie es bei zeitgenössischen Ransomware-Wellen wie *WannaCry* zu beobachten ist, ist nur ein Beispiel unter vielen, anhand dessen sich das dem IT-Sicherheitsdiskurs ebenso wie der medizinischen Immunität eigene »Paradigma einer Logik der Steigerung« (Deuber-Mankowsky 2017b, 38) ausdrückt. Mit Sybille Krämer (2008, 149) lässt sich feststellen: »Computerwürmer regen zur ›Heilung‹ – oder sollen wir sagen: zur ›Immunisierung‹ – von Betriebssystemen an.« Diese Immunisierung von Betriebssystemen besteht in ebenjener Überbietungslogik zwischen Hacker_innen und Softwareindustrie. Es stellt sich dennoch die Frage, ob nicht andere Formen von Sicherheit für die Nutzung vernetzter Systeme denkbar wären. In den nächsten Kapiteln soll der Diskussion dieser Frage nachgegangen werden, indem zunächst anhand von Backdoors eine Umdeutung des hier analysierten homophoben HIV/AIDS-Diskurses unternommen wird, und im Anschluss daran einige Überlegungen zu *Queer Computation* vorgestellt werden.

4. Backdoors

Ein Phänomen, das ein nicht zu unterschätzendes, aber oft leises Problem für die Sicherheit innerhalb digitaler Kulturen darstellt, und in der vorliegenden Untersuchung bisher nur am Rande gestreift wurde, sind Backdoors. Backdoors, auch Hintertüren genannt, sind vor allem im Kontext der vorliegenden Publikation von besonderem Interesse, da die anspruchsvolleren unter ihnen an der Intersektion von IT-Sicherheit und Kryptographie anzusiedeln sind, und ihre Analyse daher die Erkenntnisse der beiden vorangegangenen Kapitel vereint. An Backdoors lassen sich Fragen nach der Sicherheit vernetzter Computer diskutieren, die in den beiden vorangegangenen Kapiteln bereits jeweils als einem negativen Sicherheitsbegriff folgend definiert wurde. Der erste Teil dieses Kapitels wird zunächst eine informatische Definition von Backdoors vorstellen. Fragen, die dabei im Vordergrund stehen, sind: Welche Phänomene werden als Backdoor bezeichnet? Was macht eine Backdoor zu einer Backdoor? Muss immer eine Absicht hinter einer Backdoor stecken, oder können Backdoors auch unabsichtlich entstehen? Diese Fragen werden anhand von zwei Backdoors erörtert: einer verhältnismäßig trivialen *hard-coded credentials*-Backdoor und der im Zuge der Snowden-Enthüllungen zu großer Bekanntheit gelangten kleptographischen Backdoor im Pseudozufallsgenerator *DUAL_EC_DRBG*. Diese Fallbeispiele wurden ausgewählt, da sie im innerfachlichen Diskurs der IT-Sicherheit recht bekannt sind, und somit über eine gute Quellenlage verfügen, was durchaus nicht der Regelfall für Backdoors ist.

Der zweite Teil des vorliegenden Kapitels widmet sich skizzenhaft den mit Backdoors verbundenen Metaphern der Tür, der Hintertür und des Geheimnisses, und wie diese das Phänomen der Backdoor innerhalb digitaler Kulturen situieren. Im Anschluss daran wird mit der Backdoor-Schadsoftware *Back Orifice* das Verhältnis von informatischen zu menschlichen Hintertüren untersucht – also das Verhältnis von Backdoors zum Anus, sowie der homopho-

be Subtext dieses Metaphernzusammenhangs. Dieser in der Informatik eher ignorierte Zusammenhang wird unter Bezugnahme auf Guy Hocquenghem, einem Vertreter der Gay Theory der 1970er Jahre, ins Sprechen gebracht. Im Anschluss daran werden mit Leo Bersani und Paul B. Preciado zwei mögliche Lesarten von *Back Orifice* angeboten, mit denen die im vorangegangenen Kapitel herausgearbeitete Homophobie, die den IT-Sicherheitsdiskurs über die HIV/AIDS-Metaphorik informiert, denaturalisiert und/oder umgedeutet werden kann.

4.1 Was sind Backdoors?

Unter dem Stichwort »backdoor« werden in der zweiten Ausgabe des *Oxford English Dictionary* drei mögliche Bedeutungen in zwei Kategorien aufgelistet: »1.) a) A door at the back of a building or enclosure, as opposed to the front-door; a secondary or private entrance. b) back-door trot (figurative); also spec., diarrhœa,[1] dialect. 2.) figurative; also attributive = Unworthily secret, clandestine« (Oxford English Dictionary 1989). Hier besteht bereits ein Zusammenhang zwischen den hinteren, von öffentlichen Orten wie einer Straße aus nicht einsehbaren Orten der Hintertüren von Häusern, von privaten Eingängen, und der Idee der Heimlichkeit oder des Verbergens. Eine informatische Bedeutung wird nicht aufgeführt, obwohl in der Online-Ressource auch jüngere Aktualisierungen des Wortes vermerkt sind. Auch im Duden kommt diese Bedeutungsdimension nicht vor: Es gibt keinen Eintrag zu »Backdoor«, und unter dem Lemma »Hintertür« werden als Bedeutungen lediglich »1. hintere [Eingangs]tür (besonders eines Hauses, Gebäudes)« sowie »2. versteckte Möglichkeit, etwas auf nicht [ganz] einwandfreien Wegen und Umwegen zu erreichen, sich einer Sache zu entziehen« (Dudenredaktion 2018) gelistet. In der Open Access-Variante des *Oxford Dictionary* namens *Lexico* findet sich nach den bereits genannten Erklärungen auch eine kurz gehaltene informatische Bedeutung: »A feature or defect of a computer system that allows surreptitious unauthorized access to data« (Lexico 2021a). Eine Backdoor im informatischen Sinne kann also ein Feature oder ein Defekt sein, das oder der einen heimlichen und

1 Über den Bedeutungszusammenhang des Ausdrucks »back-door trot« als Bezeichnung für Durchfall wird eine Beziehung des Wortes Backdoor zum Anus/Rektum hergestellt, auf die später noch eingegangen wird.

unautorisierten Zugang zu Daten ermöglicht. Der Informatiker David Ferbrache (1992, 3) gibt in seinem Handbuch *A Pathology of Computer Viruses* folgende knappe Definition:

> »A software feature programmed by the original designer which will permit him [sic!] to carry out operations denied to normal users of the software (e.g. a login program which will accept the designer's hard-wired password irrespective of the contents of the system password file).«

Während Ferbrache die Frage nach dem un/autorisierten Zugriff ausspart, fällt die Definition im *Jargon File*, dem Wörterbuch der Hacking Culture, etwas ausführlicher aus. Dort wird darauf hingewiesen, dass der Zugang zu Daten nicht immer unautorisiert erfolgen muss, beispielsweise könnte ein_e Techniker_in eine Fernwartung mittels Backdoor durchführen. Unter dem Lemma »back door« ist dort nachzulesen:

> »A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers. Syn. trap door; may also be called a wormhole.«[2] (The Jargon File o.J.b)

Elementarer Teil dieser Definition ist die Absicht, die hinter einer Backdoor stecken muss. Während über die treibenden Motive keine Aussage getroffen wird, muss doch mindestens eines vorhanden gewesen sein, denn ohne eine Intention des_der Autor_in wird eine gegebene Sicherheitslücke laut *Jargon File* jedenfalls nicht als Backdoor klassifiziert. Im *Jargon File* (ebd.) heißt es weiter: viele Backdoors »lurked in systems longer than anyone expected or planned«, und dass nur wenige Backdoors zu größerer Bekanntheit gelangt seien. Auf welche Art eine Backdoor in ein System kommen kann, beantwortet die Definition des *Bundesamts für Sicherheit in der Informationstechnik* (BSI o.J.a), die folgendermaßen lautet:

> »Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (›Hin-

2 Die Bezeichnung *trap door* ist außerhalb des Jargon File eher in umgangssprachlichem Gebrauch, aber nicht in wissenschaftlicher Literatur zu finden. *Trap door* bezieht sich in letzterer eher auf mathematische Vorgänge, die schwer oder nicht reversibel sind (vgl. Diffie/Hellman 1976, 652). *Wormhole* hat sich als Synonym nicht durchgesetzt.

> tertür‹) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt.«

Diese Definition folgt grundsätzlich der Richtung der bereits besprochenen, besteht allerdings erneut auf einen unautorisierten Zugang, der durch eine Backdoor entsteht. Während die bisher aufgeführten Definitionen von Backdoors im informatischen Sinne zwar einen gemeinsamen Kern besitzen, unterscheiden sie sich doch in ihrer Schwerpunktsetzung, und ergeben erst in ihrer Aneinanderreihung ein ganzheitlicheres Bild. Eine umfassende Definition dessen, was eine Backdoor im informatischen Sinne sein könnte, die aus einem wissenschaftlichen Kontext kommt, ist erstaunlich schwer zu finden. Der Begriff wird eher in populärwissenschaftlichen Glossaren auf IT-Dienstleistungswebseiten erläutert als in Fachliteratur, obwohl er ständig verwendet wird.[3] Es scheint also innerhalb von IT-Sicherheit als wissenschaftlicher Disziplin eher ein intuitives Wissen davon zu geben, was eine Backdoor ist, eine Art Gebrauchsdefinition. Ferbrache (1992, 3) bemerkt dazu bereits Anfang der 1990er Jahre: »A feature of the anti-virus community has been the adoption of a wide range of (often conflicting) terminology […]«. Diesen Umstand der ausbleibenden und/oder ungenauen Definitionen adressieren auch Sam Thomas und Aurélien Francillon (2018, 93) nahezu 30 Jahre später in ihrem Aufsatz *Backdoors: Definition, Deniability and Detection*: »The term ›backdoor‹ is generally understood as something that intentionally compromises a platform, aside from this, however, there has been little effort to give a definition that is more rigorous.« Im Wesentlichen führen sie zwei Gründe für das bisherige Ausbleiben einer rigorosen Definition an. Zum einen nennen sie die Vielgestaltigkeit von Backdoors: »[…] backdoors can take many forms, and can compromise a platform by almost any means; e.g., a hardware component, a dedicated program or a malicious program fragment.« (Ebd.) Zum anderen sei eine generalisierende Definition auch aufgrund weniger bekannter und damit auch dokumentierter Backdoors schwer aufzustellen: Bei komplizierteren Backdoors habe man mit einem »sheer lack of real-world samples« (ebd.) zu kämpfen, wohingegen die bisher dokumentierten Fälle eher simpel seien und hauptsächlich darauf basierten, dass User_innen »certain static data, e.g., hard-coded credentials« (ebd.) eingeben. Solche Varianten seien zwar bereits wissenschaftlich aufgearbeitet worden, decken laut Thomas und Francillon

3 Gesucht wurde sowohl nach »backdoor« als auch nach »back door« und »Hintertür«.

(vgl. ebd.) jedoch nur einen kleinen Teil der möglichen Fälle ab. Ein Beispiel für *hard-coded credentials*[4] als Backdoor wäre folgender Fall: Änderungen am BIOS[5] eines Computers, also der Einheit, die den Computer funktionsfähig macht, können in der Regel nur nach Eingabe eines Passworts vorgenommen werden. Dieses Passwort lässt sich in den meisten Fällen von den User_innen selbst setzen, es gibt aber auch einige Standardpasswörter für verschiedene BIOS-Modelle, die auch unabhängig davon, ob die Nutzer_innen des jeweiligen Computers ein anderes Passwort eingestellt haben, noch funktionieren. Im Lauf der Zeit wurden verschiedene Passwortlisten im Internet veröffentlicht (vgl. Caloyannides 2004, 251), die es beispielsweise Hacker_innen leicht machten, unautorisiert an verschiedensten Computern Änderungen vorzunehmen.[6] Ein aktuelles Beispiel ist das *Mirai*-Botnet,[7] das erstmals 2016 in Erscheinung trat, und im selben Jahr zu internationaler Bekanntheit gelangte, da der *Mirai*-Quellcode für einen großskaligen Angriff verwendet wurde. *Mirai* suchte online nach Internet of Things-Geräten mit einem ARC-Prozessor. Auf diesem läuft eine Linux-Variante als Betriebssystem, und falls die Standardwerte für User_innenname und Passwort nicht verändert wurden, konnte *Mirai* das Gerät infizieren (vgl. Cloudflare o.J.b). Infizierte Geräte suchten selbständig nach weiteren Geräten, um auch diese mit Schadsoftware zu bespielen (vgl. BSI o.J.b). All dies geschah ohne das Wissen und/oder Einverständnis der Besitzer_innen – also *heimlich*. Zu internationaler Bekanntheit

---

4 Als »credentials« werden Zugangsdaten bezeichnet, die sowohl User_innennamen als auch Passwörter umfassen. »Hard-coded« bedeutet in diesem Zusammenhang, dass diese Daten fest im Code eines jeweiligen Systems hinterlegt sind, und nicht verändert und/oder entfernt werden können, ohne die Software selbst zu verändern.

5 Das BIOS (kurz für *Basic Input Output System*) vermittelt zwischen Hard- und Software, da es die Hardwarekomponenten eines Computers ansteuert (vgl. Schimpf et al. 2001, 75–76). Da das BIOS spezifisch auf eine jeweilige Hardware zugeschnitten ist, muss es das Betriebssystem nicht sein.

6 Auf diesen Listen finden sich nicht nur (erwartbarer Weise) die Namen der Herstellerfirmen, sondern auch absurdere Passwörter: Mehrere BIOS-Modelle der Firma *Award* können unter anderem mit dem Passwort »LKWPETER« (entweder ausschließlich in Groß- oder in Kleinbuchstaben) entsperrt werden (vgl. Caloyannides 2004, 251).

7 Als Botnet bezeichnet man ein Netzwerk aus verschiedenen Endgeräten, die mittels Schadsoftware verbunden und dann für Cyberangriffe instrumentalisiert werden. Durch die Verbindung einer großen Anzahl an Geräten (die dann als *Bots* oder manchmal auch als *Zombies* bezeichnet werden) zu einem Netzwerk werden großskalige Angriffe möglich, wie bspw. Distributed Denial of Service-Angriffe.

gelangte *Mirai*, da es mehrere hunderttausend Internet of Things-Endgeräte (darunter beispielsweise Videorecorder, Webcams, Router, Kühlschränke etc.) verbinden und eine Distributed Denial of Service-Attacke auf den DNS-Provider *Dyn* ausführen konnte, im Zuge derer weite Teile des Internets für mehrere Stunden nicht mehr zu erreichen waren (vgl. Kühl/Breitegger 2016; Schneier 2018). Zentral für die Möglichkeit, ein so riesiges Botnet aufzubauen, war ebenfalls die Tatsache, dass viele IoT-Geräte über unveränderliche *hard-coded credentials* verfügen, die als Backdoor fungiert haben, über die sich *Mirai* Zugang zu den Geräten verschaffen konnte (vgl. Weidenbach/vom Dorp 2020, 17–18).

Obgleich Thomas und Francillon (2018, 93) wiederholt von »backdoor-like functionality« sprechen, denken sie Backdoors nicht als bloße Modi oder Funktionsweisen, sondern durchaus als spezifische strukturierte Objekte, die aufgrund ihrer Vielgestaltigkeit erst durch eine Betrachtung aus verschiedenen Blickwinkeln und auf verschiedenen Ebenen trennscharf zutage treten. Zu diesem Zweck entwickeln sie ein komplexes Klassifizierungssystem, das im Weiteren schrittweise vorgestellt wird.[8] Das System fokussiert sich ausschließlich auf informationstechnologische Aspekte, stellt aber für die weiterführenden Betrachtungen eine gute Basis dar. Um die Definition nachvollziehen zu können, ist zuvor etwas Begriffsarbeit notwendig: Die Autoren setzen den Begriff *platform* als höchste Abstraktionsebene eines gegebenen Geräts, das mit einer Backdoor versehen werden soll, und ein *system* als die höchste Abstraktionsebene einer Einheit innerhalb einer *platform* (vgl. ebd., 95). Ein *system* kann beispielsweise ein Programm, ein bestimmter Teil einer Software- oder eine Hardwarekomponente sein (vgl. ebd.). Um dies anhand eines bereits bekannten Beispiels zu veranschaulichen: Ein PC wäre die *platform*, innerhalb derer das *system* BIOS den Ansatzpunkt für eine *hard-coded credentials*-Backdoor bildet. Der erste Teil der umfassenden und rigorosen Definition, die Thomas und Francillon (ebd., 98, Herv. i.O.) aufstellen, lautet folgendermaßen:

> »***Backdoor***. An *intentional* construct contained within a system that serves to compromise its expected security by facilitating access to otherwise privileged functionality or information. Its implementation is identifiable by its

8 Ein elementarer Teil von Thomas' und Francillons theoretischem Framework ist es auch, ein System zur Entdeckung von Backdoors bereitzustellen. Da dieser Part für die hier angestellten Überlegungen nicht relevant ist, wird er ausgeklammert.

> decomposition into four components: *input source*, *trigger*, *payload*, and *privileged state*, and the intention of that implementation is reflected in its complete or partial (e.g., in the case of bug-based backdoors) presence within the DFSM and AFSM, but not the EFSM of the system containing it.«

Die vier genannten Komponenten stellen laut den Autoren die Minimalbedingungen dafür dar, ein Phänomen als Backdoor zu klassifizieren (vgl. ebd.). Sie beschreiben gleichzeitig den zeitlichen Ablauf der Funktionsweise einer Backdoor: Aus einer *input source* (Eingabequelle) muss ein *trigger* (Auslöser) kommen. Wenn der *trigger* erfolgt ist, wird der *payload* (die funktionsgebende Software) ausgeführt, wonach sich das *system* im *backdoor-activated state* befindet, was bedeutet, dass die Entität,[9] die die Backdoor aktiviert hat, nun höhere Privilegien innerhalb des Systems hat als vorher, weswegen dieser Zustand auch als *privileged state* bezeichnet wird (vgl. ebd., 97). Die Frage nach der Intentionalität wird bei Thomas und Francillon durch die Modellierung verschiedener Betrachtungsperspektiven gelöst. Sie schlagen vor, dass ein gegebenes *system* von zwei entgegengesetzten Positionen betrachtet werden könne: die der Endanwender_innen und die der Entität, die die Backdoor implementiert hat (vgl. ebd., 96). Um innerhalb dieser Gegenüberstellung präzise Aussagen treffen zu können, definieren sie vier verschiedene Sichtweisen oder Versionen desselben *systems*: 1.) die Version der Entwickler_innen (developer) *DFSM*, 2.) die tatsächliche (actual) Version *AFSM*, die beispielsweise eine käuflich zu erwerbende Software ist, 3.) die von Endnutzer_innen erwartete (expected) Version *EFSM*, und 4.) die Version, die durch *Reverse Engineering*[10] erstellt wurde *RFSM* (vgl. ebd.).[11] Thomas und Francillon verwenden

---

9 Der Verständlichkeit halber wird »entity« mit Entität übersetzt, da es sich dabei sowohl um einzelne Entwickler_innen als auch um Institutionen handeln könnte, um Zufälle, Bugs oder Hacker_innen, oder um Geräte mit Schadsoftware (wie bspw. im Fall von *Mirai*).

10 Als *Reverse Engineering* wird ein Vorgang bezeichnet, bei dem eine Software, deren Quellcode unbekannt ist, anhand des ausführbaren Programms nachprogrammiert wird, sodass dieselbe Funktionalität entsteht. Da es mehrere Möglichkeiten gibt, eine konkrete Funktionalität zu erzeugen, können sich der Originalquellcode und der *Reverse Engineering*-Quellcode deutlich voneinander unterschieden.

11 Das Kürzel FSM steht für *finite state machine*, also einen *Endlichen Automaten*. Ein endlicher Automat zeichnet sich dadurch aus, dass er eine endliche Menge an Zuständen annehmen kann und zu jedem gegebenen Zeitpunkt in einem genau definierten Zustand existiert (vgl. Schimpf et al. 2001, 45–46). Nach einer Eingabe, die eine Zustandsveränderung auslöst, nimmt der Automat einen neuen Zustand aus der Menge zur Ver-

dieses Modell, um den zeitlichen Ablauf der Funktionsweise von Backdoors vereinfacht zu veranschaulichen. Dieser lässt sich exemplarisch anhand des bereits eingeführten BIOS-Beispiels nachvollziehen: Innerhalb der *platform* PC befindet sich das *system* BIOS. Das BIOS befindet sich in Zustand A. Aus der Eingabequelle Tastatur (*input source*) erfolgt nun ein *trigger* (z.B. die Passphrase »LKWPETER«), woraufhin der *payload* ausgeführt wird, und das System die Zugriffsrechte verändert. Das BIOS befindet sich im Anschluss daran in Zustand B, im *privileged state*, in dem die vor dem Computer sitzende Person mit Admin-Rechten auf das BIOS zugreifen und sensible Einstellungen verändern kann. Ob eine Backdoor nun mit Absicht in ein System integriert wurde oder nicht, lässt sich Thomas und Francillon (ebd., 106) folgend mit einem vergleichenden Blick verschiedener Versionen des gegebenen Systems feststellen. Sie schlagen drei Abstufungen vor: Eine mit Absicht eingebaute »*Intentional Backdoor*« muss ihnen zufolge mindestens teilweise in der Entwickler_innenversion (DFSM) nachweisbar sein, und der Übergang von *trigger* zu *payload* muss explizit im Quellcode erkennbar sein. Eine »*Deniable Backdoor*« wäre zum Beispiel ein Bug, der eine für User_innen unerwünschte Funktionalität bereitstellt. Diese Backdoor sei von einem rein technischen Standpunkt aus von einer unabsichtlichen Sicherheitslücke nicht zu unterscheiden, eine dahinterstehende Absicht könne jedoch aus einer gesellschaftlichen Betrachtung heraus vermutet werden. Sie kann in der DFSM nicht definitiv nachgewiesen werden, ist jedoch in der AFSM und der RFSM präsent. Eine »*Accidental vulnerability*« hingegen verfüge zwar über eine Backdoor-ähnliche Funktionalität, wird von Thomas und Francillon nicht mehr als Backdoor klassifiziert, da es weder technische noch soziale Anzeichen für eine Intentionalität gebe. Diese letzte Variante ist in der AFSM und eventuell in der RFSM, aber nicht in der DFSM präsent. Keine Backdoor oder Sicherheitslücke ist jemals in der von Endnutzer_innen erwarteten (expected) Version EFSM vorzufinden – ansonsten wäre der jeweilige Mechanismus einfach eine Funktionalität unter anderen (vgl. ebd., 107) und die Komponente der Heimlichkeit nicht mehr gegeben. Eine *hard-coded credentials*-Backdoor ist Thomas und Francillon (ebd., 106) zufolge immer eine mit Absicht eingebaute Backdoor – an dieser Stelle lässt sich hinzufügen, dass das zwar grundsätzlich stimmt, da diese auf jeden Fall von den Entwickler_innen hinterlegt worden sein muss. Dennoch lässt sich die Intention nicht genau klassifizieren: In manchen Fällen kann

fügung stehender Zustände an. Ein simples Beispiel für einen endlichen Automaten wäre eine Verkehrsampel.

eine solche Backdoor angelegt worden sein, um die Software im Entwicklungsprozess schnell bearbeiten zu können, und es wurde lediglich vergessen, diesen Zugang zu entfernen, als das Produkt veröffentlicht wurde. So liegt zwar eine Absicht vor, die aber nicht grundsätzlich darauf abzielen muss, die Entwickler_innen gegenüber den Endanwender_innen in einer privilegierten Position zu halten, und die sich ggf. lediglich auf die DFSM bezieht, aber nicht auf die anderen Versionen, da sie hätte entfernt werden sollen – dies wurde auch bereits in der Definition des *Jargon File* angesprochen. Zusammenfassend lassen sich Backdoors unter Rückgriff auf Thomas' und Francillons Klassifizierungssystem also als Phänomene beschreiben, die die erwartete Sicherheit eines Systems kompromittieren, indem sie den Zugang zu Informationen oder Funktionen, die auf einer höheren Ebene als die eines Standardnutzer_innenkontos liegen, erleichtern. Backdoors müssen mindestens über die vier Komponenten *input source*, *trigger*, *payload* und *privileged state* verfügen. Sie müssen mit Absicht angelegt worden sein, was sich über partiale Perspektiven aus der Sicht von Entwickler_innen und Nutzer_innen auf ein gegebenes System nachweisen lässt. Auf diesem Wege nicht nachweisbare Backdoor-ähnliche Phänomene werden nicht als Backdoor klassifiziert. Im Folgenden soll nun anhand der kleptographischen Backdoor in DUAL_EC_DRBG eine Backdoor vorgestellt werden, die auf einem kryptographischen Verfahren basiert. Die Funktionsweise dieser Backdoor steht in starkem Kontrast zu einer *hard-coded credentials*-Backdoor, was illustrativ für die Spannweite der Materialitäten von Backdoors verstanden werden kann.

4.1.1 Die kleptographische Backdoor in DUAL_EC_DRBG

> »Random numbers are critical for cryptography: for encryption keys, random authentication challenges, initialization vectors, nonces, key-agreement schemes, generating prime numbers and so on. Break the random-number generator, and most of the time you break the entire security system. Which is why you should worry about a new random-number standard that includes an algorithm that is slow, badly designed and just might contain a backdoor for the National Security Agency.« (Schneier 2007)

Mit diesen Worten beginnt ein im November 2007 erschienener Artikel des Security-Experten Bruce Schneier im Magazin *Wired*, in dem Schneier eine mögliche Backdoor in einem Pseudozufallszahlengenerator namens DUAL_EC_DRBG bespricht. Schneiers Ausführungen beziehen sich auf einen im

August 2007 von Dan Shumow and Niels Ferguson, zwei bei *Microsoft* angestellten Kryptographen, gehaltenen Vortrag auf der *Crypto conference* in Santa Barbara. Der kurze Vortrag mit dem Titel *On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng*[12] fand in einer informellen *rump session*[13] statt und sorgte für Aufsehen. Ihren Ausführungen zufolge war die Möglichkeit einer mathematischen Backdoor in DUAL_EC_DRBG gegeben (vgl. Bernstein et al. 2015, 8). DUAL_EC_DRBG wurde 2005 durch das *National Institute of Standards and Technology* (NIST) erstmals publiziert (vgl. ebd., 5) und 2007 durch dasselbe ratifiziert (vgl. Sullivan 2014). Das Akronym löst sich folgendermaßen auf: DRBG bezeichnet einen *Deterministic Random Bit Generator*, also einen deterministischen Algorithmus, der Zufallszahlen erzeugt. DUAL_EC steht dafür, dass die Erzeugung der Zufallszahlen auf elliptischen Kurven (Elliptic Curves) geschieht, und zwar mittels zweier (DUAL) Punkte *P* und Q, die beide auf derselben Kurve liegen (vgl. Bernstein et al. 2015, 8). Wer die Konstanten *P* und *Q* erzeugt hat, so Shumow und Ferguson, könne anhand einer Pseudozufallszahl, die durch DUAL_EC_DRBG berechnet wurde, auf die zukünftig folgenden Ergebnisse des Algorithmus schließen (vgl. ebd.). Wie Bernstein, Lange und Niederhagen (ebd.) resümieren: »obviously a security disaster.« Dennoch ließ diese Aussage auch zunächst einige Dinge ungeklärt. Bezugnehmend auf die Ergebnisse von Shumow und Ferguson konstatiert Schneier (2007), es sei trotz der mathematisch bewiesenen Möglichkeit, dass DUAL_EC_DRBG eine Backdoor enthalte, unmöglich, mit Sicherheit zu sagen, ob ein sogenannter »skeleton key«, also ein Generalschlüssel, tatsächlich existiere. Darüber hinaus weist Schneier darauf hin, dass es nicht nur unmöglich sei, mit Sicherheit zu sagen, *ob* jemand im Besitz dieses Generalschlüssels sei, sondern darüber hinaus auch, *wer* ihn besitze – die NSA, NIST oder ein_e andere_r Akteur_in? Und obwohl es darüber hinaus technisch möglich sei, DUAL_EC_DRBG so zu implementieren, dass die bekannte Backdoor ausgeschlossen werde, plädiert Schneier (ebd.) dafür, »[to] not […] use Dual_EC_DRBG under any circumstances.« Nach einer kurzen Abwägung verschiedener Details des Falles schreibt Schneier (ebd.) weiter: »If this story

12 Das Akronym PRNG bezeichnet einen *Pseudo Random Number Generator* – also einen Algorithmus zur Generierung von Pseudozufallszahlen. PRNG und DRBG werden im vorliegenden Fall oft synonym verwendet, wobei DRBG etwas spezifischer ist als PRNG.

13 *Rump sessions* oder auch *lightning talks* sind ein beliebter Teil technisch-mathematischer Konferenzen und zeichnen sich durch ihren prägnanten (oft haben die Vortragenden nur wenige Minuten Zeit) und informellen Charakter aus.

leaves you confused, join the club.« Dieser Verwirrung wird im Folgenden auf den Grund gegangen, denn mittlerweile ist der Fall DUAL_EC_DRBG von Daniel Bernstein, Tanja Lange und Ruben Niederhagen, auf deren Ergebnisse ich mich in diesem Unterkapitel maßgeblich beziehen werde, ausführlich aufgearbeitet worden.

Sicherheit und Zufall

Wie kommt eigentlich Verschlüsselung in Software? In der Regel entwickeln Kryptograph_innen Verschlüsselungsverfahren in der Form von Algorithmen, die auf derzeit schwer oder nicht lösbaren mathematischen Problemen basieren. Softwareentwickler_innen implementieren diese Algorithmen dann in Kryptographie-Bibliotheken[14] (englisch: cryptography libraries), um die bis dahin nicht anwendungsbezogene Mathematik[15] in eine Art Software-Baustein auf dem Weg zur Einbindung in spezifische Anwendungen zu verwandeln. Wieder andere Softwareentwickler_innen bauen dann diese Bibliotheken in ihre Programme ein (vgl. Bernstein et al. 2015, 3–4). DUAL_EC_DRBG ist ein solches, in der Kryptographie-Bibliothek *BSAFE* der Firma *RSA Security* enthaltenes, kryptographisches Modul.

Zeitgenössische Kryptographie beruht, wie bereits in Kapitel 2 ausführlich dargestellt, auf dem *Kerckhoffs'schen Prinzip*, das (stark verkürzt) besagt, dass die Sicherheit eines kryptographischen Verfahrens allein von dem verwendeten Schlüssel abhängen dürfe, und dass alle weiteren Komponenten des Verschlüsselungsvorgangs bekannt sein können müssen. Die Wahl eines guten Schlüssels ist daher umso wichtiger – denn wer den Schlüssel kennt oder erraten kann, kann auch die Verschlüsselung brechen. In digitalen Medien muss aus diesem Grund auch der Art, wie ein Schlüssel erzeugt wird, besondere Aufmerksamkeit geschenkt werden. An diesem Punkt kommt der

---

14 Bekannte Bibliotheken sind u.a. *OpenSSL*; *BSAFE* von *RSA Security* oder *SChannel* von Microsoft.

15 In Gesprächen mit dem Kryptographen Benedikt Auerbach machte dieser mir klar, dass die Aufgabe von Kryptograph_innen oftmals darin besteht, mathematische Verfahren zu entwickeln, die keinerlei Bezug zu Fragen der Implementierung haben. Diese sei ein nachgelagertes Problem, das andere Fachbereiche betreffe. Aus einer um Nachhaltigkeit bemühten Perspektive ergibt dies durchaus Sinn: Software verändert sich stetig, und würden Verschlüsselungsverfahren speziell auf bestimmte Anwendungsfälle zugeschnitten werden, wäre an Langlebigkeit nicht zu denken. Darüber hinaus erleichtert eine solche strikte Aufteilung der Zuständigkeiten, also eine Modularisierung verschiedener Teile derselben Software, die Fehlersuche.

Zufall ins Spiel: Computer verwenden Random Bit Generators (auch als Random Number Generators bezeichnet), um eine lange, zufällige Zahlenreihe zu erzeugen, die dann beispielsweise zur Schlüssel- oder Passwortgenerierung verwendet wird. Die Form des Zufalls, die hier gefordert ist, ist nicht derselbe Zufall, den man beispielsweise mit dem einmaligen Werfen eines sechsseitigen Würfels verbindet: Statistisch gesehen sind die Häufigkeiten gewürfelter Zahlen vorhersagbar, und jede stochastisch berechenbare Zufälligkeit wäre nachteilig für ein kryptographisches System, dessen komplette Sicherheit von dieser einen Komponente abhängt (vgl. Cloudflare o.J.a). Gesucht wird also eine Sorte nicht mittels Wahrscheinlichkeitsberechnung kalkulierbaren Zufalls, der als »true randomness« (Bernstein et al. 2015, 3) bezeichnet wird. Solche nicht vorhersagbaren Zufallszahlen sind in logikbasierten rechnenden Umgebungen schwer zu finden, daher wird das bisschen »true randomness« (ebd.), das in einem Computer gefunden werden kann,[16] mittels eines Algorithmus, der als Pseudozufallszahlengenerator bezeichnet wird, ›gestreckt‹. Dieser Algorithmus ist insofern deterministisch, als alle Ergebnisse des Pseudozufallszahlengenerators berechnet werden können, wenn der tatsächlich zufällige Input bekannt ist (vgl. ebd.). Daher wird der tatsächlich zufällige Input, auch als *seed* bezeichnet, stets geheim gehalten. Um aus Ergebnissen des Pseudozufallszahlengenerators keine Rückschlüsse auf den *seed* ziehen zu können, entspricht der Algorithmus des Pseudozufallszahlengenerators einer Einwegfunktion (vgl. Sullivan 2014). Im Fall von DUAL_EC_DRBG erfolgt die Berechnung von Pseudozufallszahlen auf sogenannten *elliptischen Kurven*. Diese verfügen über die mathematische Besonderheit, dass zwei beliebige Punkte P und Q auf einer gegebenen Kurve miteinander addiert einen Wert ergeben, der ebenfalls auf der Kurve liegt. Dies erlaubt es, die Multiplikation eines Punktes P mit einer ganzen Zahl Z als eine Z-fache Addition des Punk-

---

16 *True randomness* bei Computern wird oft durch die Eingaben von User_innen erzeugt, bspw. durch Bewegungen der Maus oder durch Tastatureingaben. Doch auch andere Dinge außerhalb des Computers können zu tatsächlichen Zufallszahlen werden: Die Firma *Cloudflare* verwendet eine Wand aus ca. 100 Lavalampen, da die Formen, die das Wachs in ihnen annimmt, nicht vorhersagbar sind. In regelmäßigen Abständen wird ein Foto von der Wand gemacht. Da digitale Fotos auch als Zahlenkolonnen ausgegeben werden können, entspricht jedes Bild einer tatsächlich zufälligen Zahlenreihe (vgl. Cloudflare o.J.a).

tes *P* mit sich selbst zu definieren.[17] Diese Multiplikation lässt sich schnell berechnen, ist allerdings auch eine Kandidatin für eine Einwegfunktion – ihre Umkehrung in Polynomialzeit berechnen zu können würde bedeuten, dass das diskrete Logarithmusproblem auf elliptischen Kurven gelöst worden wäre (vgl. ebd.). Die in DUAL_EC_DRBG mathematisch beweisbare Backdoor hängt mit genau dieser Einwegfunktion zusammen, und den zuvor erwähnten zwei Punkten *P* und *Q*, die beide auf derselben elliptischen Kurve liegen, und als Konstanten in die Berechnung von Pseudozufallszahlen eingehen, indem sie mit einem *seed* jeweils in eine Einwegfunktion eingesetzt werden. Die Backdoor in DUAL_EC_DRBG besteht darin, dass, wer die Beziehung der Konstanten *P* und Q zueinander kennt, oder genauer: wer weiß, wie *P* aus der Multiplikation von Q gewonnen werden kann, in der Lage ist, von einer durch DUAL_EC_DRBG erzeugten Zahl aus alle weiteren Pseudozufallszahlen, die DUAL_EC_DRBG produzieren wird, zu errechnen (vgl. Bernstein et al. 2015, 8, 12). Dem Framework von Thomas und Francillon folgend, besteht zu diesem Zeitpunkt der Analyse eine *deniable backdoor*: Shumows und Fergusons Überlegungen wurden anhand der AFSM angestellt, und die EFSM enthielt selbstverständlich keine Backdoor, denn immerhin wurde DUAL_EC_DRBG vom *National Institute of Standards and Technology* veröffentlicht und ratifiziert. Mathematisch nachweisbar ist, dass es möglich wäre, anhand der Kenntnis der Beziehung der Konstanten *P* und Q zueinander mittels eines einzigen Outputs aus DUAL_EC_DRBG alle weiteren Outputs zu berechnen. Es ist jedoch nicht zwingend notwendig, *P* und Q auf eine Weise zu erzeugen, die eine Backdoor generieren würde. Unklar ist also, ob diese mathematische Backdoor in der DFSM vorhanden ist, also ob die Entwickler_innen von DUAL_EC_DRBG tatsächlich über diesen Generalschlüssel verfügen.

Tatsächlich eine *deniable backdoor*?

Shumow und Ferguson waren sehr darum bemüht, ihrem Fund keine Intentionalität zu unterstellen. Entsprechend liest sich die vorletzte Folie ihrer Präsentation:

> »WHAT WE ARE NOT SAYING: NIST intentionally put a back door in this PRNG

17 P+P+P=Q entspricht 3xP=Q. Es handelt sich hier um das mathematische Verfahren der sog. Gruppenoperation, das aus Gründen der Verständlichkeit entweder als Addition oder Multiplikation beschrieben werden kann.

> WHAT WE ARE SAYING: The prediction resistance of this PRNG (as presented in NIST SP800-90) is dependent on solving one instance of the elliptic curve discrete log problem. (And we do not know if the algorithm designer knew this before hand [sic!].)« (Shumow/Ferguson 2007)

Thomas und Francillon (2018, 106) verweisen in ihrer Definition einer *deniable backdoor* darauf, dass im Fall einer technisch nicht nachweisbaren Backdoor in der DFSM stattdessen »from a non-technical perspective«, also aus einer Betrachtung politischer Zusammenhänge, einer Entität eine Intentionalität unterstellt werden könne. Aus heutiger Perspektive hätten Shumow und Ferguson guten Gewissens eine Intentionalität unterstellen können, allerdings nicht NIST, sondern der NSA: In dem 2006 von NIST veröffentlichten Dokument namens SP 800–90 für DUAL_EC_DRBG werden keine Erfinder_innen des Pseudozufallszahlengenerators benannt (vgl. Bernstein et al. 2015, 6). Als die Autor_innen des Dokuments, Elaine Barker und John Kelsey, eine Anfrage bezüglich eines möglichen Kommentars zu DUAL_EC_DRBG erhielten, leitete Elaine Barker diese Mail an Mitarbeiter_innen der NSA weiter, mit dem Hinweis, dass diese die Frage beantworten könnten (vgl. ebd.), woraus deutlich hervorgeht, dass die NSA für die Entwicklung von DUAL_EC_DRBG verantwortlich ist. Aus einem 2014 veröffentlichten Mailwechsel zwischen John Kelsey (NIST) und Don Johnson (NSA) aus dem Jahr 2004, in dem Kelsey nach dem Ursprung der Konstanten *P* und Q fragt, ist weiterhin ersichtlich, »that NSA had ›generated (*P*, Q) in a secure, classified way‹ […] and that it ›would be reasonable to allow other users to generate their own (*P*, Q)‹.« (Ebd., 9) In einem Appendix zu SP 800–90 riet NIST jedoch explizit davon ab, eigene Konstanten zu erzeugen, um die Integrität der Verschlüsselung nicht mit unter Umständen falsch gewählten Konstanten zu beschädigen (vgl. ebd.). Bernstein, Lange und Niederhagen (ebd., 10) resümieren: »In hindsight it is quite amazing how blindly NIST trusted NSA.« Doch damit noch nicht genug. Anfang 2005 brachte die kanadische Firma *Certicom* zwei Patente auf den Weg: eines für die Verwendung der DUAL_EC_DRBG-Backdoor für *key escrow*,[18] und eines für eine

18 Unter *key escrow* versteht man das Hinterlegen eines Schlüssels für ein Kryptosystem bei einer Regierung oder einem Geheimdienst etc. Bernstein et al. (2015, 20) bezeichnen dies als »deliberate back door«. Bei *key escrow* besteht jedoch immer die Gefahr des Missbrauchs des hinterlegten Schlüssels. Eine mögliche Lösung für dieses Problem kommt vom David Chaum. Das von ihm vorgestellte System »Privategrity« beinhaltet ein *key escrow*-Verfahren, bei dem der Schlüssel, mit dem eine Kommunikation entschlüsselt werden kann, in neun Teile gesplittet wird und jedes Teil in einem anderen

Modifikation von DUAL_EC_DRBG, die *key escrow* unmöglich macht (vgl. ebd., 20). Anhand dieser beiden Patente lässt sich belegen, dass *Certicom* bereits im Jahr 2005 von der Backdoor im DUAL_EC_DRBG wusste, und die NSA spätestens im April 2005 ebenfalls über die Backdoor informiert war (vgl. ebd.). Darüber hinaus waren die Unterlagen für die Patentierung inklusive Beispiele für den Exploit von DUAL_EC_DRBG im Juli 2006 im Internet auffindbar – und das nur einen Monat nach der Standardisierung von DUAL_EC_DRBG als SP 800–90 durch NIST (vgl. ebd.). Darum bemüht, Aufsehen ob dieser Patente und der Backdoor in DUAL_EC_DRBG zu vermeiden, listete auch *Certicom* zwei Namen vermutlich unbeteiligter Personen als Erfinder der Patente.

Tatsächlich sollte es noch bis kurz nach den Snowden-Enthüllungen dauern, bis die Standardisierung und Verwendung von DUAL_EC_DRBG international größeres Aufsehen erregte. Aus einem Bericht vom 06.09.2013 in der Zeitung *The Guardian*, die über mehrere Artikel hinweg die von Edward Snowden bereitgestellten Dokumente journalistisch aufarbeitete, geht hervor, dass die NSA gemeinsam mit dem britischen Geheimdienst GCHQ seit einigen Jahren systematisch an einer Schwächung kryptographischer Systeme arbeitete, um abgefangenen Traffic entschlüsseln und mitlesen zu können. Das entsprechende Projekt trägt den Titel *Bullrun* (das britische Äquivalent trägt den Namen *Edgehill*) und ist Teil des SIGINT-Programms (vgl. Ball et al. 2013), das dem offensiven Teil der NSA zugeordnet ist. Das Ziel von SIGINT wird in internen Dokumenten der NSA folgendermaßen beschrieben:

> »The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact.« (National Security Agency 2012, 115)

Land liegt (vgl. Greenberg 2016). Nur wenn alle Schlüsselparteien von der Notwendigkeit einer Entschlüsselung überzeugt sind, fügen sie ihre Teile zu dem vollständigen Schlüssel zusammen und entschlüsseln die Kommunikation. Auf diese Weise möchte Chaum einen leichtfertigen Gebrauch des Master-Schlüssels verhindern, aber gleichzeitig Regierungen die Möglichkeit geben, Terrorismus zu bekämpfen (vgl. ebd.) – ein scheinbar ausgewogener Kompromiss aus Privacy und Security.

Anhand dieser Absichtserklärung lässt sich erneut die von Thomas und Francillon vorgenommene Differenzierung der Nachweisbarkeit von Backdoors in DFSM und EFSM beobachten: die Backdoors sollen, wenn möglich, nur in der DFSM enthalten, und im besten Fall auch dort nicht explizit nachweisbar sein. Ball, Borger und Greenwald (2013) weisen darauf hin, dass *Bullrun* explizit darauf abzielt, »to ›insert vulnerabilities into commercial encryption systems‹.« In den Dokumenten werden zwar keine Firmen explizit benannt (vgl. Menn 2013), jedoch ist durch eine Meldung der Nachrichtenagentur Reuters nur wenige Monate nach Bekanntwerden von *Bullrun* ersichtlich, dass die NSA 10 Millionen US-Dollar an die Firma *RSA Security* zahlte, um DUAL_EC_DRBG zum standardmäßig voreingestellten Pseudozufallszahlengenerator in *RSAs* Kryptographie-Bibliothek *BSAFE* zu machen (vgl. Ars Staff 2013; Menn 2013; Sullivan 2014).[19] Bernstein, Lange und Niederhagen (2015, 2) bemerken dazu: »The surprise for the public cryptographic community was not so much this confirmation of what had already been suspected, but rather that NSA's backdooring of Dual EC was part of an organized approach to weakening cryptographic standards.« Auf ein Element der Politiken dieses organisierten Vorgehens wird im folgenden Abschnitt eingegangen.

»NOBUS«

»You look at a vulnerability through a different lens if even with the vulnerability it requires substantial computational power or substantial other attributes and you have to make the judgment who else can do this?«, sagte Michael Hayden, ein ehemaliger Direktor der NSA, auf dem *Washington Post Cybersecurity Summit* im Oktober 2013, rund einen Monat nachdem im *Guardian* über *Bullrun* berichtet wurde. Er führte weiter aus:

> »If there's a vulnerability here that weakens encryption but you still need four acres of Cray computers[20] in the basement in order to work it you kind of think »NOBUS« and that's a vulnerability we are not ethically or legally compelled to try to patch – it's one that ethically and legally we could try to

19 Dies bedeutet zwar nicht, dass irgendjemand zu dessen Verwendung verpflichtet wäre – Softwareentwickler_innen, die sich nicht mit Kryptographie auskennen, würden aber vermutlich den ihnen vorgeschlagenen Standard verwenden, da sie keine informiertere Entscheidung treffen können. Genau diese Kompetenz sollte ihnen durch die Existenz von Kryptographie-Bibliotheken immerhin abgenommen werden.

20 »Cray computers« ist eine Bezeichnung für Supercomputer, die auf den Markennamen des bekanntesten Herstellers derselben verweist.

exploit in order to keep Americans safe from others.« (Hayden in Peterson 2013)

Die Abkürzung »NOBUS« steht für »nobody but us« und bezieht sich in Haydens Statement konkret auf die monetären und rechnerischen Ressourcen der NSA im Vergleich zu denen anderer Akteur_innen. Diese Einschätzung kann als eine Auslegung von David Kahns (1967, 753) Aussage verstanden werden, das Verhältnis von Kryptographie zu Kryptanalyse sei maßgeblich von Zeit geprägt: Mit dem Zusammenwachsen von Kryptologie und Informatik treten Rechenleistung und monetäre Ressourcen in eine Wechselbeziehung zu verfügbarer Zeit. Die NSA-interne Klassifizierung von Sicherheitslücken gelte, so fügt Hayden erläuternd hinzu, sowohl für bereits existierende, aus zufälligen Fehlern entstandene, absichtlich implementierte oder nachträglich zu Überwachungszwecken eingesetzte Sicherheitslücken (vgl. Peterson 2013). Doch bei DUAL_EC_DRBG handelt es sich um einen Sonderfall, bei dem sich Kryptographie und Kryptanalyse nicht im konventionellen Sinne gegenüberstehen: Der erste Schritt besteht, Adam Young und Moti Yung (1997) folgend, in »Using Cryptography Against Cryptography«. Diese Tagline ist ein Teil des Titels von Youngs und Yungs Paper über *Kleptographie*. Kleptographie definieren Young und Yung (ebd., 63) als »the ›study of stealing information securely and subliminally‹«,[21] und exemplifizieren: »The kleptographic attacker can steal the secrets securely, and in an exclusive and subliminal manner.« Während Youngs und Yungs Konzept der Kryptovirologie, wie in Kapitel 3 bereits besprochen wurde, die Möglichkeit beschreibt, mittels Verschlüsselung einen Angriff auszuführen, bei dem den Angegriffenen Zugang versperrt und Daten vor ihren Besitzer_innen erpresserisch zurückgehalten werden können, beschreibt Kleptographie die Möglichkeit, Kryptographie gegen sich selbst zu wenden, sodass eine verwendete Verschlüsselung für alle außer der kleptographisch operierenden Entität sicher und vertrauenswürdig erscheint. Bezugnehmend auf eine ihrer früheren Arbeiten beschreiben Young und Yung dies anhand eines mit dem Akronym SETUP benannten Algorithmus. SETUP steht für »Secretly Embedded Trapdoor with Universal Protection«, und ein solcher Algorithmus »can be embedded within a cryptosystem to leak encrypted secret key information to the attacker in the output of that cryptosystem.« (Ebd., 64) Der SETUP-Algorithmus wird als einem

21 Bei Kleptographie lassen sich durchaus Anklänge an steganographische Verfahren bemerken.

gegebenen kryptographischen System zugehörig beschrieben, es erfolgt also weder ein Angriff durch ein Außen, noch muss eine zusätzliche (und ansonsten verräterisch überflüssige) Komponente in ein *system* integriert werden, die die zu schützenden Informationen preisgibt. Es ist also die Implementierung von SETUP selbst, die »in conjunction with the internal cryptographic tools, *generates* opportunities for leaking information.« (Ebd., 63, Herv. i.O.) Dies führt zu einer Situation, in der, ähnlich wie bei DUAL_EC_DRBG, nur die Entität, die die Beziehung der Konstanten *P* und Q zueinander kennt, den Output des Pseudozufallszahlengenerators entschlüsseln und zukünftige Kombinationen berechnen kann. Im Fall einer kleptographischen Backdoor kann also nur die Entität, die SETUP implementiert hat, auch etwas mit den geleakten Informationen anfangen, da diese verschlüsselt sind. Mehr noch: Nur die Entität, die SETUP implementiert hat, weiß überhaupt, dass ein *system* Informationen preisgibt. Basierend auf diesem Konzept lässt sich die *deniable Backdoor* in DUAL_EC_DRBG durch das Vorgehen der NSA als *kleptographische* Backdoor einstufen. Die Backdoor in DUAL_EC_DRBG ermöglicht es der NSA also, Daten »in an exclusive and subliminal manner« zu stehlen, da sie – in Schneiers (2007) Worten – den »skeleton key« besitzen, diese Sicherheitslücke aber für andere Akteur_innen aufgrund des diskreten Logarithmusproblems auf elliptischen Kurven nicht ausnutzbar ist. Ob dies auch »securely« geschieht, ist vom Blickwinkel abhängig: Da kein_e NSA-Agent_in sich dafür in eine physisch gefährliche Situation begeben muss, und die Daten für alle nicht eingeweihten Akteur_innen weiterhin verschlüsselt sind, könnte man davon ausgehen, dass die NOBUS-Politik der NSA in kleptographischen Backdoors ihr volles Potential entfaltet, und maximale Überwachung bei maximaler Sicherheit gewährleistet. Diese Auffassung lässt sich angesichts rezenter Cyberangriffe wie *WannaCry* allerdings auch als schlichtweg falsch beschreiben: Die Sicherheitslücke *EternalBlue* in *Windows*' SMB-Protokoll war der NSA zum Zeitpunkt von *WannaCry* bereits seit einigen Jahren bekannt, wurde jedoch im Zuge der NOBUS-Einschätzung nicht publik gemacht, um sie weiter ausnutzen zu können. Auf diese Weise konnte die NSA zwar über einige Jahre hinweg operieren, aber schlussendlich schadete diese Sicherheitslücke, als sie durch die *Shadow Brokers* im Internet veröffentlicht wurde, auch den Vereinigten Staaten massiv – der von Hayden formulierte Anspruch »to keep *Americans* safe from others« (Peterson 2013, Herv. MS) wurde also in letzter Konsequenz nicht eingelöst. Ein ähnliches Schicksal könnte auch eine kleptographische Backdoor treffen: Würde der geheime Schlüssel, mit dem Q generiert wurde (vgl. Bernstein et al. 2015,

8–9), gestohlen und veröffentlicht werden, würde die Backdoor nicht mehr exklusiv der NSA zur Verfügung stehen. Einmal veröffentlicht, wäre die Ausgabe jeder einzelnen DUAL_EC_DRBG-Instanz mit den Standardwerten für *P* und Q vorhersagbar (vgl. Schneier 2007).

Die absichtliche Schwächung kryptographischer Infrastrukturen durch aktives Eingreifen oder durch gezielte Passivität ist jedoch kein neues Phänomen. Bruce Schneier (2018) legt in *Click here to kill everybody* dar, dass bereits seit den 1990er Jahren immer wieder Verschlüsselung von verschiedenen geheimdienstlichen Organisationen als unüberwindbare Hürde zur Verfolgung krimineller Akteur_innen diskursiviert wurde. Die wiederholt zur Rechtfertigung solcher Forderungen vorgebrachten Akteur_innen »terrorists, drug dealers, pedophiles, and organized crime« bezeichnet Schneier (ebd.) aufgrund des repetitiven Diskurses scherzhaft als die »Four Horsemen of the Internet Apocalypse«. Er plädiert, wie viele andere Wissenschaftler_innen aus den Bereichen IT-Sicherheit und Kryptographie, sowie FLOSS[22]-Aktivist_innen, für kompetentere Ermittlungsstrategien statt der Ausweitung technologischer Kompetenzen der Geheimdienste. Denn, so Schneiers (ebd.) Argument:

> »While in theory it would be great [...] there's no way to design this securely. It's impossible to build a backdoor mechanism that only works in the presence of a legal warrant, or when a law enforcement officer tries to use it for legitimate purposes. Either the backdoor works for everyone or it doesn't work for anyone.«

4.2 Von Türen, Hintertüren und Schlüsseln

Nachdem im vorangegangenen Unterkapitel zwei Arten von Backdoors, sowie ein informatisches Framework für die Bestimmung von Backdoors besprochen wurden, wird im Folgenden auf die in dem Begriff »Backdoor« als Metapher enthaltene Tür eingegangen. In Kapitel 3 wurde IT-Sicherheit vor allem in Bezug auf Sicherheit vor Schadsoftware besprochen, doch die Herstellung von Sicherheit bei Computern verfügt noch über einen weiteren

22 Das Akronym FLOSS steht für Free, Libre and Open Source Software und fasst so unterschiedlich lizensierte Software, deren Quellcode in jedem Fall frei einsehbar ist, zusammen.

Bereich. Wie Parikka (2016, 3) ausführt, basieren »security and computer protection [...] on *control*, *inspection*, and *integrity*.« Während *inspection* und *integrity* mit dem Auffinden von Schadsoftware und unautorisierten Veränderungen innerhalb eines Computers befasst sind, kommt *control* eine umfassendere Rolle zu: »As the key concept of computer security, it has meant controlling access to systems, as well as functions, resources, and the moving and sharing of data.« (Ebd.) Das offensichtlichste Beispiel für die Herstellung von Sicherheit durch *control* ist an *access control*, also Zugangs- oder Zugriffskontrolle orientiert: Bei der Verwendung eines Computers ist der_die User_in in den meisten Fällen mit Lese- und Schreibrechten für die meisten Dateien auf der Festplatte ausgestattet. Um alle Dateien, darunter auch die, die die Programme und Funktionen des Computers ausmachen, lesen und bearbeiten zu dürfen, wird in der Regel ein Passwort abgefragt. Dies soll verhindern, dass aus Versehen oder von unbefugten Personen oder Programmen Änderungen am System vorgenommen werden und dieses dadurch in einen Zustand veränderter oder reduzierter Funktionalität versetzt wird, oder dass jemand unrechtmäßigen Zugang zu Informationen erlangt. Bei den Betriebssystemen *Microsoft Windows*, *MacOS* und *Ubuntu* ist dies das Passwort, das der_die User_in auch verwendet, um sich in seinem_ihrem Account anzumelden: Der_die User_in muss nachweisen, dass er_sie autorisiert ist, Änderungen an bestimmten Dateien vorzunehmen.[23] Die Abfrage eines Passworts vor dem *Betreten* eines bestimmten Bereichs ist ein Vorgang der Authentifizierung: Das Passwort fungiert also wie eine Losung, wie ein *Schlüssel*, wie ein geteiltes *Geheimnis* zwischen User_in und Computer, mit dem eine Person nachweisen kann, dass sie wirklich über die Berechtigung verfügt, einen abgegrenzten Bereich zu betreten, dort Dokumente anzusehen und zu bearbeiten. Bei Sicherheit als Zugangskontrolle funktioniert die Frage nach dem Passwort wie eine *Tür*, das Passwort wie der dazugehörige *Schlüssel*: Der Authentifizierungsmechanismus steht wie eine Tür zwischen zwei Bereichen, gewährt bei korrekten Eingaben den Übertritt in einen geheimen oder privaten Bereich, und bringt diesen, ebenso wie ihr öffentlicheres Gegenstück gleichsam durch die Grenzziehung erst hervor.

---

23 Das Betriebssystem *Debian* hingegen verlangt standardmäßig ein anderes Passwort als das des_der User_in, und differenziert auch explizit zwischen *user* und *root user*, wobei Root-User_innen Lese- und Schreibberechtigungen für alle Bereiche des Computers haben.

Türen und Hintertüren

In seinem Aufsatz *Türen. Zur Materialität des Symbolischen* widmet sich Bernhard Siegert (2010) aus kulturtechnischer Perspektive den Beziehungen zwischen Menschen und Türen als Objekten des Alltags. Die vorliegende Publikation hat sich bereits methodisch gegen eine kulturtechnische Herangehensweise positioniert, dennoch lässt sich Siegerts Text an dieser Stelle für die Analyse von Backdoors produktiv machen. Siegert legt anhand von unterschiedlichen Türsorten eine Art Motivgeschichte der Tür vor: Glastüren, Drehtüren und Schiebetüren, sowie die *Porte de Duchamp*[24] werden bedacht, lediglich Hintertüren erwähnt er leider nicht. »Türen«, so schreibt Siegert (ebd., 153–154), seien »Operatoren symbolischer, epistemischer und sozialer Prozesse, die mithilfe der Differenz zwischen innen und außen Rechtssphären, Geheimnissphären und Privatsphären generieren, wodurch sie den Raum so artikulieren, dass er zum Träger kultureller Codes wird.« Diese Definition versteht Türen als Elemente der Differenzgenerierung. Angesichts der im vorangegangenen Kapitel herausgearbeiteten immunologischen Struktur des IT-Sicherheitsdiskurses scheint sich die Metapher der Tür damit zunächst nur allzu passend als eine weitere Spielart der »frontier-based concepts« (Taylor 2001, 38) neben Metaphern der Landnahme und des Immunsystems begreifen zu lassen. Dieser Eindruck mag jedoch täuschen: Obwohl Siegert sich nur in stark verkürzter und nahezu naiver Weise über Türen digitaler Medien äußert,[25] schwingt jedoch ein Prinzip des Digitalen in seinen Betrachtungen mit: die Binarität. Dies ist beispielsweise dort erkennbar, wo er zu der Tür Duchamps schreibt: »Die Tür als digitales Medium bezieht sich auf die Passage von Körpern.« (Siegert 2010, 160) Nun ließe sich argumentieren, dass die Tür Duchamps ohnehin mit Binarität befasst, und Siegerts Analyse daher äußert treffend sei. Doch auch an anderer Stelle orientiert er sich an naturwissenschaftlichem Wissen, und überträgt dieses auf die Betrachtung von Türen aus Holz, beispielsweise in seiner Betrachtung eines Auszugs aus

24 Die *Porte de Duchamp* ist ein Entwurf des Künstlers Marcel Duchamp, die mit drei Räumen operiert, von denen sie stets zwei miteinander verbindet und einen dritten schließt (vgl. Siegert 2010, 158–159).

25 Siegerts (2010, 165) Behauptung, dass »in den virtuellen Architekturen des Cyberspace, des Internet […] die Differenz von innen und außen dekonstruiert und permanent aufgeschoben« würde, muss als das Festhalten an einer nicht eingelösten Utopie des Internets eingestuft werden. Die vorliegende Publikation sollte – neben zahllosen weiteren – mittlerweile mehr als deutlich gemacht haben, dass die Differenz von Innen und Außen gerade in digitalen Kulturen bis heute grundlegend ist.

Robert Musils Geschichte *Türen und Tore.* In dem von ihm zitierten Ausschnitt Musils schreibt dieser über die Rolle von Türen für die un/gleiche Verteilung von Wissen, die in neueren Häusern nicht mehr gegeben sei, da die Wände dieser so dünn seien, dass man nicht mehr an der Tür zu lauschen brauche – man könne bereits alles durch die Wände hören (vgl. ebd., 163). Siegert (ebd.) hält jedoch an der Rolle der Tür als Differenz generierend fest, wenn er schreibt:

> »So lange Türen ihre Rolle spielten als Operatoren der Differenz zwischen innen und außen schufen sie auch – mithilfe der Differenz zwischen öffentlich und privat – eine Asymmetrie im Wissen. Türen produzieren ein Informationsgefälle. Sie spielen daher eine unverzichtbare Rolle in der Produktion thermodynamischen bzw. informationstheoretischen Wissens. […] Solange Türen ihre informatische Funktion erfüllen, halten sie ein Energie- bzw. Wissensungleichgewicht aufrecht, das ein Anwachsen der Entropie im Gesamtsystem nahezu unvermeidlich macht. Auf diese Weise dienen Türen der Wissenszirkulation […].«

Die Tür kann, wenn sie, wie hier bei Siegert, digital und damit binär gedacht wird, entweder geöffnet oder geschlossen sein, eine halboffene Tür kann es nicht geben. Damit erweist sich die Tür mehr als eine Verabsolutierung von Differenz denn als eine aushandelnde Differenzgenerierung, die im Gegensatz zum Immunsystem nicht die Logik der Steigerung, sondern die der Binarität verkörpert. In der Übertragung der Tür als Metapher für informatische Formen der Regulierung von Informationsaustausch, so lässt sich anhand von Siegert feststellen, büßt die Tür die Möglichkeit ein, angelehnt zu werden, nur halb geschlossen zu sein, und wird zu einer binären Unterscheidungsmaschine, die entweder geöffnet oder geschlossen ist, Zutritt gewährt oder verweigert. So schreibt auch Bruno Latour (1996, 69) in *Ein Türschließer streikt*: »Im Jargon der Informatik: Eine Tür ist ein ausschließendes ODER, niemals ein UND«. Dies gilt bei Computern für Türen in Hardware (sog. Gates, dt.: Gatter) und in Software. Was passiert aber mit der Binarität, wenn es nicht nur eine Tür gibt? An dieser Stelle kommt die Hintertür ins Spiel, denn mit einer Reihe von Türen lassen sich, um zunächst in einer technischen Beschreibungsweise zu bleiben, differenziertere Schaltungen erzeugen, ähnlich einem gemischten Stromkreis, der aus Reihen- und Parallelschaltungen konstruiert ist. ›Türen‹ bei Computern erzeugen Ein- und Ausschlüsse binärer Art, die von heimlich angebrachten weiteren Türen störend erweitert werden können. So wirken beispielsweise kleptographische Backdoors an der Aufrechterhaltung

der grundsätzlichen Struktur des Informationsgefälles dadurch mit, dass sie einen Zugang zu einem geschützten Bereich ermöglichen, und diesen Zugang wiederum selbst mittels kryptographischer Verfahren schützen – dennoch verändern sie das Informationsgefälle zugunsten der User_innen, die durch die Backdoor gewissermaßen ›eintreten‹. So bringen Backdoors die vorgegebene Unterscheidung von Innen und Außen in Gefahr, weil sie eine zweite Eintrittspforte schaffen, wo nur eine sein sollte. An der Binarität der Tür-Metapher in der Informatik ändert dies allerdings nichts.

Schlüssel und Geheimnis

Zu den Türen und Hintertüren gehört, wie eingangs erwähnt, auch stets ein *Schlüssel*, das heißt, ein Passwort, ein *Geheimnis*. Das Geheimnis, oder vielmehr, das Verraten eines Geheimnisses, hat vor allem in den letzten Jahren durch zahllose Whistleblower_innen und Enthüllungen eine prominente Position in digitalen Kulturen eingenommen. Timon Beyes und Claus Pias (2014, 111) weisen in ihrem Aufsatz *Transparenz und Geheimnis* darauf hin, dass es unter den gegebenen Umständen sinniger sei, digitale Kulturen »nicht, oder nicht primär, in Potential und Problematik der Transparenz (und korrespondierender Leitbegriffe wie Partizipation und Öffentlichkeit) zu denken, sondern im Zeichen des Geheimen, der fundamentalen Intransparenz und des Arkanums.« Die Autoren führen die privilegierte Stellung des Geheimnisses auf die Vormachtstellung der modernen Kybernetik seit 1945 zurück, die eine neue Form von Zeitlichkeit etabliert habe (vgl. ebd., 114), die durch die fortschreitende Digitalisierung unserer Lebenswelt zur Normalität geworden sei. Sie fassen Algorithmen, die als *black box* operieren, als Kennzeichnungsmerkmal dieser neuen Zeitordnung, die die Zukunft nicht mehr offenhalte, sondern schließe – als Paradigmenwechsel führen sie anhand der Klimaforschung an, nicht mehr die Natur sei das Geheimnis, das es zu entschlüsseln gelte, sondern die Datenverarbeitung (vgl. ebd., 116). In einer Umkehrbewegung rücken Beyes und Pias (vgl. ebd., 112) mit Bezug auf Eva Horn anstelle von Transparenz Partizipation und Öffentlichkeit in den Vordergrund:

> »Die Frage ist nicht, was geheim gehalten wird, sondern was überhaupt verraten werden kann, und was – indem es zum Objekt des Verrats werden kann oder nicht – den Stellenwert und die Logik des Geheimnisses in verschiedenen Kulturen und zu verschiedenen Zeiten ausmacht.«

Kryptologie kommt in Beyes' und Pias' Paper nicht vor, dennoch lässt sich basierend auf den bisher erfolgten Überlegungen anmerken, dass nicht nur

die Kybernetik und die durch sie entstandenen Algorithmen für die von Beyes und Pias diagnostizierte Verschiebung verantwortlich zu zeichnen haben. Die Geschichte der Kryptologie, und damit auch die spätestens seit der Entschlüsselung der Enigma mit ihr verknüpfte Geschichte der IT-Sicherheit, drehen sich um die Möglichkeit der Geheimhaltung und damit, in derselben Umkehrbewegung, um die Frage danach, was überhaupt verraten werden kann. Die Verwaltung des Geheimen, die von so vielen Autor_innen als eine Militärgeschichte erzählt wird, da sie eng mit Belangen der Kriegsführung verbunden war, betrifft in nicht unmittelbaren Kriegssituationen vermittelt über Geheimdienste die Relationen von Staaten zueinander, aber auch die von Bürger_innen zu ihren Staaten (vgl. Sprenger 2016). Kryptographie nach dem Kerckhoffs'schen Prinzip lässt sich zugespitzt formuliert als die Verwaltung von Geheimnissen (Plaintext) mittels Geheimnissen (Schlüsseln) beschreiben. Backdoors lassen sich in diesem Sinne als Tropen verstehen, die Teil dieser komplexen Relationen sind, und mit denen der Status des Geheimnisses verändert werden kann, wie anhand von DUAL_EC_DRBG expliziert wurde. Darüber hinaus veruneindeutigt sich das Vokabular selbst an den Stellen, wo die verschiedenen Metaphern, die zur Beschreibung des Phänomens herangezogen werden, sich überlappen: Eine *hard-coded credentials*-Backdoor besteht, wie bereits ausgeführt, darin, dass in einem gegebenen System eine Art General*schlüssel* hinterlegt wird, mit der eine Entität sich immer Zutritt zu diesem verschaffen kann. Die Hinter*tür* kann also auch darin bestehen, ein *Schlüssel* zur Vordertür zu sein. Das nun folgende Unterkapitel widmet sich der sexualisierten Dimension der Backdoor-Metapher, die in den vorherrschenden Diskursen der Informatik übersehenen oder als Ausnahme abgetan wird, und wie diese mit *Gay Theory* ins Sprechen gebracht werden kann.

4.3 ›In through the back door…‹: Mögliche Umdeutungen

In der bereits zitierten aktuellen Online-Ausgabe des *Oxford English Dictionary* wird darauf verwiesen, dass der Eintrag »backdoor« noch nicht für die dritte Ausgabe des OED bearbeitet wurde. Allerdings wird eine weitere Bedeutung als »Draft Addition« aufgeführt: »*slang*. The anus, the rectum« (Oxford English Dictionary 2021). Der erste gelistete Verwendungsnachweis für diesen Wortsinn reicht bis ins Jahr 1613 zurück, zu dem Theaterstück *The Insatiate Countess*

von John Marston.[26] In einer Szene des Stücks unterhalten sich zwei weibliche Nebencharaktere, Thais und Abigail, über ihre zukünftigen Ehemänner. Diese kommen aus zwei verfeindeten Familien und wollen die bestehende Familienfehde selbst in der ›doppelten‹ Hochzeitsnacht aufrechterhalten (beide Paare sollen am selben Tag heiraten). Statt ihre Fehde im Kampf auszutragen, beschließen die Männer allerdings, die Frau des jeweils anderen zu verführen. Thais und Abigail, die befreundet sind, möchten diesen Plan mit ihrem eigenen durchkreuzen: Indem sie die Häuser tauschen, soll in der doppelten Hochzeitsnacht jede von ihnen mit ihrem jeweiligen Ehemann Sex haben. Teil des Gesprächs sind folgende Zeilen:

> »*Abig*. […] The hour for both to come, is six; a dark time, fit for purblind lovers; and with cleanly conveyance by the nigglers our maids, they shall be translated into our bed-chambers: your husband into mine, and mine into your's.
> *Thais*. But, you mean they shall come in at the back-doors.
> *Abig*. Who? our husbands? nay, an they come not in at the fore-doors, there will be no pleasure in't. But, we two will climb over our garden-pales, and come in that way; (the chastest that are in Venice will stray, for a good turn;) and thus wittily will we be bestowed: you into my house, to your husband; and I into your house, to my husband; and, I warrant thee, before a month come to an end, they'll crack louder of this night's lodging than the bedsteads.« (Marston 1820, 31–32)

Abigails Bemerkung, »nay, an they come not in at the fore-doors, there will be no pleasure in't«, lässt sich sowohl auf die Tatsache beziehen, dass die beiden Männer dahingehend getäuscht werden sollen, dass sie durch die Vordertür in das jeweilige Haus eintreten können, um symbolisch die Oberhand behalten zu haben (die Heimlichkeit des Eintretens durch die Hintertür wird hier zugunsten einer offen sichtbaren Dominanzgeste ausgetauscht), als auch darauf, dass Abigail eine pikante Bemerkung darüber macht, dass anale Penetration im Gegensatz zur vaginalen keine Freude bereite. Eine Hintertür findet sich in diesem Dialog also sowohl an Häusern als auch an Körpern – beide werden damit jeweils als geschlossene Systeme konstituiert, mit einer Hülle (Haut/Wände), die das Innere klar von dem Äußeren abgrenzt. Eine ähnliche Mehrdeutigkeit und sexualisierte Zweideutigkeit wird dem Begriff

26 Unter den Verwendungsnachweisen finden sich weiterhin diverse Umgangssprachen-Wörterbücher sowie ein Männer-Lifestylemagazin (vgl. ebd.).

Backdoor auch im *Urban Dictionary*[27] attestiert, beispielsweise in Eintrag Nummer 9, der folgende Erklärungen listet: »1. dishonest 2. the anus 3. a malicious computer program installed to allow access by hackers and other malware«. Der 5. Eintrag präzisiert: »Refers to a person's anus in the context of anal intercourse.« Als Beispielsatz wird dort angegeben: »Sally likes it in the back door.« Auch der folgende Eintrag gibt einen ähnlichen Beispielsatz: »Tom fucked Glenda, up the back door«. In einem weiteren Beitrag wird Backdoor als »smelly brown hole« erläutert und mit dem Beispielsatz »Oi bitch do you take it up the back door« versehen. Weitere Beispielsätze beinhalten »She has a big backdoor«, »Her Back Door is so damn sexual, I just wanna grab it!«, »She has a fine back door.« Kurz, das Wort Backdoor bezeichnet im Urban Dictionary in den meisten Fällen: »A Person's Ass, mostly a female.« (Urban Dictionary o.J.). Auffällig an dieser Auflistung, aber auch am ersten Verwendungsnachweis in *The Insatiate Countess* ist, dass Backdoor als Anus, vor allem im Zusammenhang mit Analsex, in erster Linie Frauen, und auch explizit heterosexuellem Sex zugerechnet wird. Wird diese Praxis in *The Insatiate Countess* noch eindeutig abgewertet, so ist sie im *Urban Dictionary* schon nicht mehr so eindeutig negativ konnotiert, wobei an dieser Stelle auch darauf verwiesen sei, dass die meisten Beispielsätze über Frauen sprechen, und nicht aus ihrer Sicht. Expliziter Genuss seitens der Frau wird nur in einem Beispiel erwähnt. Penetrativer Analsex jenseits von als heterosexuell zu lesenden Konstellationen oder Frauen in der penetrierten Position kommt in den bisherigen Beispielen nicht explizit vor. Dies rahmt penetrativen Analsex zwar als heterosexuelle Sexualpraktik, allerdings nur durch den Ausschluss analer Penetration von Männern. Dies lässt sich durchaus als ein Symptom heteronormativer Diskurseffekte begreifen, die sich, wie bereits gezeigt wurde, auch im Bereich der IT-Sicherheit finden. Mit der folgenden Diskussion der Software *Back Orifice*, die den Zusammenfall von Backdoor und Anus expliziert, soll die ansonsten auf der Ebene des Subtexts verbleibende Homophobie der Metaphern des IT-Sicherheitsdiskurses, die bereits in den Ausführungen zur HIV/AIDS und Schadsoftware angerissen wurde, fokussiert und politisiert werden. Es stellt sich also die Frage, wie dieser Subtext, wie Fragen nach Lust, Begehren und Liebe, die bestenfalls in den Beispielen (und anekdotischen

27 Das *Urban Dictionary* ist ein Wörterbuch für Umgangssprache, sowie explizit auf digitale Kulturen bezogene sprachliche Phänomene. Es folgt einem ähnlichen Prinzip wie Wikipedia: Jede_r kann Bedeutungen beisteuern – moderiert wird allerdings weniger als bei Wikipedia.

Witzen), aber nicht in den wissenschaftlichen Schriften der IT-Sicherheit selbst thematisiert werden (vgl. Bergermann 2018, 339), ins Sprechen gebracht werden können. An dieses Unterfangen schließt sich eine weitere Frage an: Was wird sag- und denkbar, wenn die sexualisierten Zweideutigkeiten des IT-Sicherheitsdiskurses mit scheinbar randständigen Phänomenen wie *Back Orifice* in das Zentrum der Analyse gestellt werden? Diesen Fragen wird in einem argumentativen Dreischritt nachgegangen: Zunächst wird anhand eines kurzen Überblicks über *Back Orifice* die naheliegende Lesart als homophober Witz erläutert. Diese wird im nächsten Schritt kritisiert, und unter Rückgriff auf Positionen der Gay Theory zur Bedeutung des Anus und den mit ihm verbundenen Praktiken in westlichen Kulturen umgedeutet. Als dritter und letzter Schritt wird versucht, mit Queer Computing einen Gegenentwurf zum bestehenden negativen Sicherheitsbegriff der IT-Sicherheit zu entwerfen, um die dort vorhandenen Ausschlüsse nicht zu reproduzieren.

4.3.1 *Back Orifice*

Anfang August 1998 stellte die US-amerikanische Hackergruppe *Cult of the Dead Cow* auf der Hacker_innenkonferenz DEFCON (6) ein Programm namens *Back Orifice* vor. *Back Orifice* wurde offiziell als Fernwartungssoftware (englisch: remote administration tool) für *Microsoft Windows 95* angekündigt – aber »[d]aß die Intention eine andere ist, ergibt sich schon aus dem Namen«, wie auf *heise.de* im August 1998 zu lesen ist: »Back Orifice (hintere Öffnung) übersetzt man hier am besten mit ›Hintertür‹, denn das Programm macht es fast zum Kinderspiel, Schindluder mit Windows-PCs zu treiben.« (Himmelein 1998) Die Verwendung von Fernwartungssoftware ermöglicht es, einen Computer von einem zweiten Computer aus fernzusteuern, sowie die auf ihm vorhandenen Dateien auszulesen. Software dieser Art wird daher in erster Linie zu ihrem namensgebenden Zweck der Wartung aus der Ferne eingesetzt, beispielsweise wenn die Computer eines Unternehmens durch ein weiteres Unternehmen auf dem neuesten Stand gehalten oder von Schadsoftware gereinigt werden sollen. *Back Orifice* wurde allerdings nicht in einem solchen kommerziellen Setting und in gegenseitigem Einvernehmen eingesetzt, sondern eher als Scherzprogramm verwendet und ohne das Wissen der jeweiligen Personen, denen ein Streich gespielt werden sollte, auf ihrem Computer installiert. ›Hintere Öffnung‹ als Übersetzung für *Back Orifice* ist gemessen an der Verwendung des Wortes *orifice* im Englischen allerdings eine etwas zahme Übersetzung, denn *orifice* bezeichnet nicht einfach irgendwelche, sondern

spezifisch Körperöffnungen: »An opening, particularly one in the body such as a nostril or the anus« (Lexico 2021b). Computer werden, so lässt sich als erste Beobachtung festhalten, durch diese Benennung der Software einmal mehr als Körper konfiguriert. Der Name der Software ist neben diesem Wortspiel auch eine Anspielung auf das vier Jahre zuvor erschienene Produkt *Microsoft BackOffice Server*, ein Softwarepaket für Firmenkund_innen, das die Servervariante von *Microsoft Windows NT* und später *Windows 2000* sowie weitere Programme enthielt (vgl. Wikipedia 2016). In einer Pressemitteilung mit dem Titel *Running a Microsoft Operating System on a Network? Our Condolences* auf ihrer Webseite lassen *Cult of the Dead Cow* vermuten, der Urheber von *Back Orifice*, ein unter dem Pseudonym *Sir Dystic* bekannter Hacker (vgl. Wikipedia 2017), habe *Back Orifice* als eine Art pädagogische Hacking-Maßnahme im Kampf gegen »Microsoft's Swiss cheese approach to security« (Cult of the Dead Cow 1998a) geschaffen.

Anfang der 2000er Jahre warnte auch das Rechenzentrum der Ruhr-Universität Bochum vor *Back Orifice* (vgl. RUB RZ 2002), stellte eine kurze Anleitung zur Verfügung, wie *Back Orifice* zu löschen sei und verlinkte eine Webseite mit weiterführenden Informationen. Während diese Webseite durchaus sehr detailliert Auskunft über *Back Orifice* gibt, sind die Titel der einzelnen Einträge spannend: Von *The Back Orifice »Backdoor« Program. YOUR security is at risk* (Little 1999) bis zu *Almost All The Ways to Find Your Back Orifice* (Little 1998) wird deutlich, dass *Back Orifice* in den Augen des auf seiner Webseite zunächst anonym bleibenden Verfassers nicht nur Computer, sondern auch User_innen direkt betrifft, die er als »›orificed‹ people« (Little 1999) bezeichnet, die er vor *Back Orifice* gerettet habe. Die Gleichsetzung und Verbindung menschlicher und maschinischer Körper wurde bereits im vorangegangenen Kapitel ausführlich diskutiert. Die Übertragung der Gefahr von Computer auf User_innen lässt sich als ein Effekt der *Personal Systems Hygiene-* und *Safe Hex*-Diskurse werten, und mit Parikka (2016, 116) weiterhin als typisch für den IT-Sicherheitsdiskurs einordnen, in dem Computer, aber auch User_innen als »frequently gendered and sexualized with rhetorics of rape and other images of vulnerability« erscheinen. Während es naheliegend ist, aufgrund dieser Übertragung in *Back Orifice* einen langen, homophoben Witz zu sehen, und Analysen des Sexismus innerhalb der Hacking Culture (siehe exemplarisch Taylor 2001), sowie die bisherigen Erkenntnisse über den IT-Sicherheitsdiskurs eine solche Intentionalität nahelegen würden, soll an dieser Stelle eine Umdeutung versucht werden. Mit dem in der Übertragung dieser Rhetoriken von Computern auf Menschen entstandenen Ausdruck

»›orificed‹ people« wird eine weitere Dimension sicht- und adressierbar, die über die Unannehmlichkeiten dysfunktionaler Computer hinausgeht, und im Spannungsfeld dieser Übertragung besprochen werden soll: Dass eine Grenzverletzung im Bereich der IT-Sicherheit mit der Metapher eines geöffneten Körpers beschrieben wird, ist nach den bisherigen Ausführungen erwartbar. Weshalb aber verknüpft sich eine Grenzverletzung im Bereich der IT-Sicherheit und der damit einhergehende Verlust von Privatsphäre spezifisch mit der Metapher eines geöffneten Anus? Welche (negativen) Konnotationen verbinden sich mit der Bezeichnung »›orificed‹ people«? Sind nicht alle Menschen per se *orificed*, das heißt, verfügen nicht alle Menschen über Körperöffnungen, über einen Anus? Und sind nicht alle Computer erst durch (die Standardisierung ihrer) Anschlussstellen, also durch ihre Öffnungen in Hard- und Software überhaupt steuerbar? Was macht Backdoors als Figurationen innerhalb dieser Kultur so bemerkenswert? Die in der Vermischung der offenen Hintertür im Computer mit dem (offenen) Anus sichtbar werdende Verknüpfung von Penetriertwerden und einer dadurch implizierten Passivierung, die als Verlust von Sicherheit und Macht gefasst wird, soll im Folgenden befragt werden.

4.3.2 Über den Anus

Für die Diskussion des Anus abseits von heteronormativer Theoriebildung, die in der *Gay Theory* ihren Anfang nahm, werden an dieser Stelle drei Ansätze besprochen, die sich mit Analsex in einer heteronormativen, und damit homophoben Gesellschaft auseinandersetzen, aber zu unterschiedlichen Schlüssen und Konsequenzen kommen. Der erste ist Guy Hocquenghems Anfang der 1970er Jahre erschienenes Buch *Le désir homosexuel*, in dem ausgehend von der durch Hocquenghem wahrgenommenen konservativ-psychoanalytischen Ausrichtung der damaligen Gesellschaft anale Penetration als eindeutig schwule Sexualpraktik kontextualisiert, sowie der Zusammenhang des Anus und der Formation von Subjektivität und Privatheit expliziert wird. Das Projekt Hocquenghems ließe sich als der Versuch beschreiben, den von der Psychoanalyse (fehl)informierten Diskurseffekten einer kapitalistischen Gesellschaft zu entkommen, allerdings nicht, indem er die Psychoanalyse gänzlich verwirft, sondern über eine genaue Lesart und Auseinandersetzung mit ihr, sowie des Topos der Paranoia, die einen privilegierten Schauplatz für die Analyse von Homosexualität darstellt. Der zweite hier diskutierte Ansatz findet sich in Leo Bersanis Aufsatz *Is the Rectum a Grave?*, mit dem die

Diskursivierung des penetrativen Analsex homosexueller Männer im Zuge der AIDS-Krise noch einmal genauer betrachtet werden soll. Auch Bersani bezieht sich auf die Psychoanalyse, zieht aber andere Konsequenzen als Hocquenghem. Seine Forderung ist nicht, die bestehenden Strukturen zu zerschlagen, sondern den mit analer Penetration verknüpften Machtverlust, der als Passivierung diskursiviert wird, in seiner Negativität aufzuwerten. Abschließend wird anhand von zwei Texten Paul B. Preciados, *Anal Terror. Notes on the First Days of the Sexual Revolution* und *Kontrasexuelles Manifest*, eine metaphorische Umdeutung von *Back Orifice* vorgenommen. Preciado baut seine Argumentation auf Hocquenghems Analyse auf, und kommt so ebenfalls zu der Forderung, dass die heteronormative Gesellschaftsordnung zerschlagen werden müsse. Anale Penetration ist für Preciado dabei das Mittel der Wahl, denn er begreift diese als eine Praktik, mit der Körper von sexueller Orientierung und Geschlechtsidentität gelöst werden können. Preciado geht es also im Gegensatz zu Bersani nicht um eine Aufwertung der Passivität im Sinne einer Erfahrung des Machtverlusts, sondern um die Einebnung der Differenz von aktiv und passiv, und damit auch des Machtgefälles. Da Preciado in *Anal Terror* mit einem stark an die Informatik angelehnten Vokabular arbeitet, wird dieser Text als Brücke genommen, um eine Umdeutung der homophob lesbaren Metaphorik von *Back Orifice* vorzunehmen.

Sexualisierung, Paranoia, Kapitalismus

Guy Hocquenghems Buch *Le désir homosexuel*, das 1972 in Frankreich erschien, kann von heute aus betrachtet als erstes in einer Reihe von Werken gesehen werden, die eine Form des Wissens und der Wissensproduktion darstellen, die die Grundlage der Queer Theory bildet (vgl. Preciado 2015, 140). Das Buch wurde in den letzten Jahren erneut in zahlreiche Sprachen übersetzt und mit Begleittexten und einordnenden Vorworten versehen. Gemeinsam mit der spanischen Veröffentlichung mit dem Titel *El deseo homosexual* im Melusina Verlag im Jahr 2000 wurde auch ein Aufsatz Paul B. Preciados mit dem Titel *Terror anal: Apuntes sobre los primeros días de la revolución sexual* veröffentlicht, der mit Hocquenghems Text in einen Dialog tritt.[28] *Anal Terror. Notes on the First Days of the Sexual Revolution*, so der englische Titel von Preciados Essay, ist eine kurze und polemisiert zugespitzte Geschichte des Anus als Schauplatz der Herstellung von Körpern, Geschlecht und sexueller Orientierung. *Le désir homosexuel* war eine für die damalige Zeit in mehrfacher Hinsicht revolutionäre

---

28 Im Folgenden werden die englischen Übersetzungen beider Texte verwendet.

Schrift: Hocquenghem schrieb über Homosexualität und homosexuelles Begehren, ohne dieses zu pathologisieren. Preciado (ebd., 126) weist darauf hin, dass nicht nur der Inhalt, sondern auch die Form des Texts von damals ungekannter Schlagkraft war: »There are no apologies, excuses, or justifications in Hocquenghem's text. They're lacking because he no longer wants to be the good boy […].«[29] Mit Roland Barthes ordnet Preciado (ebd.) Guy Hocquenghems Buch als »textual terrorism« ein, da es das erste Buch war, in dem ein offen schwuler Mann die Verbindung von Kapitalismus und Heterosexualität untersuchte. Hocquenghem, Gründungsmitglied der *Front Homosexuel d'Action Révolutionnaire* (FHAR), arbeitet sich an der Freud'schen Psychoanalyse ab: an den Effekten der Normalisierung ihres Wissens in der Breite der kapitalistischen Gesellschaft[30] sowie den Verdrehungen, die dieses Wissen dabei erfährt. Die kapitalistische Gesellschaft, so Hocquenghem (1993, 50), »manufactures homosexuals just as it produces proletarians, constantly defining its own limits: homosexuality is a manufactured product of the normal world.« Die mit dem Begriff Homosexualität konstruierte abstrakte Kategorie des Begehrens erlaube es, Machtrelationen auch auf die Subjekte auszudehnen, die ansonsten außerhalb des Gesetzes stünden, und sei damit Teil einer Gesellschaft, die fortschreitend Menschengruppen klassifiziere und ihnen einen sozialen Status zuschreibe (vgl. ebd., 51). Elementarer Teil der Arbeit Hocquenghems ist die Denaturalisierung von Homosexualität als eine über Begehren konstruierte Identitätskategorie, indem sie als Diskurseffekt beschreibbar wird.

»The problem is not so much homosexual desire«, beginnt Hocquenghem (ebd., 49) seine Überlegungen, »as the fear of homosexuality: why does the mere mention of the word trigger off reactions of recoil and hate?« Er folgert, dass es diskursive Strategien geben müsse, die diese »reactions of recoil and hate« auslösen, und nimmt sich auf der Suche nach diesen zunächst der »Anti-Homosexual Paranoia« (ebd., 55) an. Die gesellschaftliche Diskursivierung von Homosexualität, beobachtet Hocquenghem (ebd., 56), sei »the fruit of the paranoia through which a dominant sexual mode, the family's reproductive

---

29 Peter Rehberg (2019, 101) bemerkt in seinem Essay *Energie ohne Macht. Christian Maurels Theorie des Anus im Kontext von Guy Hocquenghem und der Geschichte von Queer Theory*, es habe eine »Domestizierung von Queer« stattgefunden, die er unter anderem der Übersetzungspraxis zurechnet: »Mit der Übersetzung ins Deutsche hat die Kategorie Queer somit auch das Anstößige und Verletzende, das ihr im Englischen anhaftet, verloren.«

30 Zentral für Hocquenghems Betrachtungen zum Kapitalismus ist Gilles Deleuzes und Félix Guattaris nahezu zeitgleich erschienenes Buch *Capitalisme et schizophrénie. L'anti-Œdipe* (dt.: *Anti-Ödipus: Kapitalismus und Schizophrenie*).

heterosexuality, manifests its anxiety at the suppressed but constantly recurring sexual modes.« Diese Angst vor Homosexualität, konstatiert er, sei eine Umkehrung von Freuds Konzept der Paranoia,[31] denn »Freud's famous ›persecutory paranoia‹ is in actual fact a paranoia that *seeks to persecute.*« (Ebd., Herv. i.O.) Er schreibt weiter:

> »The reversal of meaning which Freud's concept has undergone in this respect is enlightening. Freud states that persecutory paranoia is generally connected with the repression of the libido's homosexual component. Social man's fear of his own homosexuality induces in him a paranoiac fear of seeing it appear around him.« (Ebd.)

Freuds paranoider Wahn, der also eigentlich ein *verfolgender* ist, wird in einer Umkehrbewegung von der Gesellschaft in eine Paranoia umgedeutet, die sich *verfolgt* fühle. Die Herstellung von Homosexualität als Identitätskategorie gehe daher mit ihrer Unterdrückung durch die Mehrheitsgesellschaft einher (vgl. ebd., 55). Dies wiederum manifestiere sich in einer homophoben Paranoia:

> »The attitude of what is commonly called ›society‹ is, in this respect, paranoiac: it suffers from an interpretative delusion which leads it to discover all around it the signs of a homosexual conspiracy that prevents it from functioning properly.« (Ebd.)

Was Hocquenghem hier als »homosexual conspiracy« benennt, lässt sich auch heute noch wiederfinden, beispielsweise in der Kontroverse um den Bildungsplan 2015 des Landes Baden-Württemberg, im Zuge derer eine Petition mit dem Titel *Zukunft – Verantwortung – Lernen: Kein Bildungsplan 2015 unter der Ideologie des Regenbogens* gestartet wurde, mit der verhindert werden sollte, dass auch LGBTQI*-Themen und -Lebensentwürfe im Schulunterricht behandelt werden (vgl. o.A. 2013). Die Unterdrückung von Homosexualität führe gleichzeitig zu einer »spontaneous sexualisation of all relationships with a homosexual« (Hocquenghem 1993, 55), die schließlich in der Angst münde, von of-

31 Freud diagnostizierte Daniel Paul Schrebers Paranoia als Resultat verdrängter Homosexualität: »Die Eigenart der Paranoia (oder der paranoiden Demenz) müssen wir in etwas anderes verlegen, in die besondere Erscheinungsform der Symptome, und für diese wird unsere Erwartung nicht die Komplexe, sondern den Mechanismus der Symptombildung oder den der Verdrängung verantwortlich machen. Wir würden sagen, der paranoische Charakter liegt darin, daß zur Abwehr einer homosexuellen Wunschphantasie gerade mit einem Verfolgungswahn von solcher Art reagiert wird.« (Freud 1955, 295)

fen schwulen Männern vergewaltigt zu werden. Hocquenghem (ebd., 55–56) wendet also die psychiatrische Definition von *persecutory paranoia*, die Homosexuellen zuschrieb, sich bedroht oder verfolgt zu fühlen, mit einer genauen Freudlektüre zurück in ihr (ursprüngliches) Gegenteil und kommt so zu dem Schluss, dass der vorherrschende homophobe Diskurs vielmehr selbst ein Ergebnis der Verdrängung anderer Formen von Sexualität durch die dominante reproduktive Heterosexualität sei. Ebendiese *persecutory paranoia* ist beispielhaft in der Petition gegen den baden-württembergischen Bildungsplan 2015 zu erkennen, in der beklagt wird, dass

> »die ethische Reflexion der negativen Begleiterscheinungen eines LSBTTIQ-Lebensstils, wie die höhere Suizidgefährdung unter homosexuellen Jugendlichen, die erhöhte Anfälligkeit für Alkohol und Drogen, die auffällig hohe HIV-Infektionsrate bei homosexuellen Männern, [...] die deutlich geringere Lebenserwartung homo- und bisexueller Männer, das ausgeprägte Risiko psychischer Erkrankungen bei homosexuell lebenden Frauen und Männern« (o.A. 2013)

fehle, wobei Lehrer_innen gleichzeitig gezwungen würden, »Coming-out zu neuen ›sexuellen Orientierungen‹ pädagogisch [zu] propagieren« (ebd.). Die von Hocquenghem beschriebene homosexuelle Verschwörung als »interpretative delusion« zeigt sich hier darüber hinaus in der Vermutung, es handle sich beim Bildungsplan 2015 um eine »pädagogische, moralische und ideologische Umerziehung an den allgemeinbildenden Schulen« (ebd.). Anhand dieses Beispiels wird deutlich, wie Hocquenghem mit Paranoia als zentralem Konzept operiert, das, wie Eve Kosofsky Sedgwick (2003, 126) in ihrem Aufsatz *Paranoid Reading and Reparative Reading, or, You're So Paranoid, You Probably Think This Essay Is About You* schreibt, damit zur »uniquely privileged site for illuminating not homosexuality itself, as in the Freudian tradition, but rather precisely the mechanisms of homophobic and heterosexist enforcement against it« wird. Über diese Umkehrbewegung könne Hocquenghem somit erklären, schreibt Sedgwick (ebd.) weiter, »not how homosexuality works, but how homophobia and heterosexism work – in short, if one understands these oppressions to be systemic, how the world works.«

In Hocquenghems (1993, 93) Lesart, die die von der Psychoanalyse (fehl)informierte Pathologisierung, aber auch die davor dominante Kriminalisierung von Homosexualität in Betracht zieht, sind diese beiden Modi der Verwerfung von Homosexualität verbunden mit der Herausbildung des Kapitalismus als dominanter Gesellschaftsform westlicher Zivilisation. Hocquenghem geht

insbesondere auf Freuds Konzept der *analen Phase* ein, die in einer nach Plan verlaufenden Entwicklung eines Kindes von der *genitalen Phase* abgelöst werden müsse. In letzterer ereigne sich Freud zufolge der Ödipuskonflikt, durch den Kinder sowohl Heterosexualität erlernten als auch Moral. In der Überwindung der analen Phase ereignet sich Hocquenghem (ebd., 96) folgend die von Freud formulierte »formation of the person«: Indem der Anus mit dem erfolgreichen Erwerb von Kontinenz als Lustzentrum überwunden werde, seien alle mit dem Anus verbundenen Funktionen »excremental« geworden. Bezugnehmend auf Deleuze und Guattari verknüpft Hocquenghem (ebd.) dies mit der Formation von Privatheit: »The anus has no social position except sublimation. The functions of this organ are truly private; they are the site of the formation of the person. The anus expresses privatisation itself.« Basierend auf zwei psychoanalytischen Fallanalysen[32] der Verbindung von Homosexualität und Paranoia mit besonderem Fokus auf den Anus konstatiert Hocquenghem (ebd., 98–99) unter Rückgriff auf Deleuze und Guattari, Kontrolle über den Anus sei die Vorbedingung für die Fähigkeit, Güter zu besitzen, also in die Ordnung des Kapitalismus einzutreten. Denn Geld, das zuerst in dem privaten Besitz einer Person liegen müsse, um schließlich auf dem Markt zirkulieren zu können, sei mit dem Anus als privatestem Teil des Körpers verbunden (vgl. ebd., 96–97). Vor diesem Hintergrund betrachtet, erscheinen informatische Backdoors in ihrer Zweideutigkeit als Hintertür und Anus, und die mittels Backdoors herstellbaren Grenzverletzungen als homophobes Motiv innerhalb eines heterosexistisch kodierten Systems: Bei *Back Orifice* wird die Verknüpfung analen Penetriertwerdens mit dem Verlust

32 Hocquenghem (1993, 98–99) führt einerseits einen durch den ungarischen Psychoanalytiker Sándor Ferenczi beschriebenen Fall eines bis zu einer operativen Entfernung einer Analfistel in seiner Gemeinde sehr aktiv gewesenen Bauern an, der nach der Operation einen paranoiden Verfolgungswahn entwickelte und sich aus dem Gemeindeleben ins Private zurückzog. Ferenczi diagnostiziert, die Operation durch männliche Ärzte habe eine latente, bis dahin sublimierte Homosexualität zutage gefördert, die nun dafür verantwortlich sei, dass der Bauer einen paranoiden Wahn entwickelt habe, und sich von anderen Männern fernhalte, obwohl er bis dahin ein angesehenes Mitglied der Gemeinde gewesen sei. Das zweite Fallbeispiel ist Sigmund Freuds Analyse des Falls Schreber, der konstitutiv für das Konzept von Paranoia in der Freud'schen Psychoanalyse ist, und in dem Freud verdrängte Homosexualität als Auslöser für Daniel Paul Schrebers paranoiden Wahn ausmachte. Die Unterdrückung der möglichen Verwendung des Anus als Lustzentrum spielt in beiden Analysen eine tragende Rolle, da diese Sublimierungsleistung das gesellschaftliche Ansehen beider Männer bedinge.

von Sicherheit und Privatheit deutlich ausbuchstabiert. Der geöffnete Anus eignet sich, Hocquenghem und Preciado folgend, wie keine andere Körperöffnung für diese Metapher. Die Verbindung des Anus mit dem Privaten, führt Hocquenghem (ebd., 97) weiter aus, bindet gleichsam den Phallus an die Öffentlichkeit: »The constitution of the private, individual, ›proper‹ person is ›of the anus‹; the constitution of the public person is ›of the phallus‹.« Mit Preciado (2015, 125) lässt sich zuspitzen, dass mit dieser Verwerfung des Anus der Penis als »despotic signifier« erschien, und der Phallus als »affordable mega-$-porno-fetish of the new Disney-heterosexual-land.« Körper, deren Anus im übertragenen Sinne ›offen‹ geblieben war – Preciado (ebd.) zählt dazu die Körper von Frauen und »fag bodies« – wurden konsequenter Weise von Machtpositionen ausgeschlossen und aus der Öffentlichkeit verbannt.

Penetrativer Analsex und Passivität

Zusätzlich zur Bedeutung des Anus sowie der notwendigen Überwindung der analen Phase, um in die kapitalistische Ordnung eintreten zu können, macht Hocquenghem (1993, 98) deutlich, dass Homosexualität für die Psychoanalyse nicht bloß an den Anus als Lustzentrum, sondern spezifisch an anale Penetration geknüpft sei: »Homosexuality primarily means anal homosexuality, sodomy.« Zur (bis heute) mit Analsex diskursiv verbundenen Passivierung der anal penetrierten Person konstatiert er:

> »Experience has proved the thesis that effeminate men are attracted to masculine ones and vice-versa to be quite absurd. The categorisation of so-called passive sodomy as ›effeminate‹ is not even based on the material reality of homosexual relationships, where men who are considered most masculine are surely not necessarily, nor even in the majority of cases, the ›male‹ partners.« (Ebd., 118–119)

Hocquenghem geht nach dieser Anmerkung ausführlicher auf psychoanalytische Positionen zur Objektwahl und -beziehung ein, um die Verbindung von Homosexualität und dem Weiblichen zu dekonstruieren, was an dieser Stelle jedoch nicht verfolgt werden soll. Stattdessen lässt sich hier mit Bersani (1987, 212) anschließen, der die Idee der Passivierung durch Penetration historisiert. Selbst in Kulturen, die Homosexualität per se nicht ablehnend gegenüberstanden, wie beispielsweise im antiken Rom oder der islamischen Kultur zur Zeit des Mittelalters wurde die Position des anal penetrierten Mannes abgewertet (vgl. ebd.). Mit Foucault schreibt Bersani (ebd.) über die explizite Verknüpfung von Penetration und Passivität im antiken Griechen-

land: »A general ethical polarity in Greek thought of self-domination and a helpless indulgence of appetites has, as one of its results, a structuring of sexual behavior in terms of activity and passivity, with a correlative rejection of the so-called passive role in sex.« Die damit einhergehende »legal and moral incompatibility between sexual passivity and civic authority« (ebd.) traf vor allem auf erwachsene Männer zu, und Bersani (ebd., Herv. i.O.) formuliert pointiert: »In other words, the moral taboo on ›passive‹ anal sex in ancient Athens is primarily formulated as a kind of hygienics of social power. *To be penetrated is to abdicate power.*« Im Verlauf seines Aufsatzes geht es Bersani allerdings nicht darum, die Passivität, also den Machtverlust, des_der Penetrierten in eine Aktivität umzudeuten, sondern vielmehr in ihrer Negativität zu rehabilitieren. Bezugnehmend auf Simon Watneys Formulierung des *Rektums als Grab* schreibt Bersani (ebd., 222): »[…] if the rectum is the grave in which the masculine ideal (an ideal shared – differently – by men *and* women) of proud subjectivity is buried, then it should be celebrated for its very potential for death.« Dieser Satz lässt sich folgendermaßen verstehen: Die privilegierte Position, die im Phallozentrismus dem Penis vor dem Anus (und der Vagina) zukommt, so führt Bersani (ebd., 217, Herv. i.O.) weiter aus, sei »not primarily the denial of power to women (although it has obviously also led to that, everywhere and at all times), but above all the denial of the *value* of powerlessness in both men and women.« Powerlessness bezieht sich an dieser Stelle weder auf Sanftheit noch auf Passivität, sondern auf Freuds Bemerkung, dass für das Empfinden sexueller Lust die Organisation des Selbst für eine kurze Zeit unterbrochen werden müsse (vgl. ebd.). Dieser Akt des »self-shattering« (ebd.) sei es, der Sexualität mit Machtpositionen, spezifisch mit Machtverlust, verknüpfe. Im letzten Kapitel wurde bereits ausführlicher auf die von Bersani analysierte Verbindung von homosexuellem Analsex, imaginierter und realer Promiskuität sowie pathologisierter weiblicher Sexualität eingegangen, bei der anale Penetration als eine Praktik »associated with women but performed by men« (ebd., 220) imaginiert werde, was in letzter Konsequenz homosexuelle Männer selbst zum Zeichen der HIV-Infektion, und damit des unausweichlichen Todes mache. Zusammengedacht mit dem Potential des »self-shattering« wohnt homosexuellem Analsex Bersani zufolge also eine Negativität inne, die er allerdings nicht umdeuten möchte, in der Hoffnung, dass sich auf diese Weise die Homophobie der Gesellschaft bekämpfen ließe. Bersanis Einsatz besteht vielmehr in der genau gegensätzlichen Bewegung: Wenn das Rektum als Grab des männlichen Ideals, und der damit verbundenen Machtposition imaginiert wird, dann besteht Bersani

(ebd., 222) zufolge die befreiendere Haltung darin, es »for its very potential for death« zu zelebrieren.

Was könnte dies für die Betrachtung von *Back Orifice* bedeuten? In einer affirmativen Lesart ließe sich *Back Orifice*, und damit im übertragenen Sinne das anale Penetrieren von Computern, nicht als homophober Witz, sondern vielmehr als ein lustvoller Umgang mit dem »potential for death« von Backdoors begreifen. *Back Orifice* auf dem eigenen Computer zu entdecken, könnte bedeuten, die damit einhergehende Machtlosigkeit zu genießen. Die Möglichkeit, mittels *Back Orifice*, oder Backdoors im Allgemeinen in vernetzte Computer einzudringen, ließe sich somit als lustvoller Akt einstufen, der dem in Teilen homophoben IT-Sicherheitsdiskurs mit exakt dem begegnet, was er verwirft.

Sex(ualität) als Technologie

Preciados Anliegen lässt sich quer zu Bersanis begreifen, insofern es Preciado nicht darum geht, die mit analem Penetriertwerden verbundene Machtlosigkeit aufzuwerten, sondern die Dynamiken abzuschaffen, die überhaupt erst ein solches Machtgefälle innerhalb von Sexualität erzeugen. Mit Preciado stellen sich also folgende Fragen: Wie könnte die Konzeptionalisierung analen Penetriertwerdens als passivierend der heteronormativen Deutungshoheit entzogen werden? Könnte das Praktizieren analen Penetriertwerdens, sofern es von Menschen aller Geschlechter und sexuellen Orientierungen durchgeführt würde, seinen Status im gegebenen System und dieses selbst verändern, da seine Beschreibungskategorien bereits in ihrer deskriptiven Funktion als unbrauchbar markiert werden?

Preciado widmet sich diesen Fragen mit scharf polemisierenden wissenschaftlichen Texten, sowie Anleitungen zu konkreten Arten, Sex zu haben: Ein radikales Programm, das er *Kontra-Sexualität* tauft. Das Anliegen von Kontra-Sexualität, formuliert Preciado (2003, 10), »handelt nicht von der Erschaffung einer neuen Natur, sondern vom Ende einer Natur, die als Ordnung verstanden wird und die Unterwerfung von Körpern durch andere Körper rechtfertigt.« Diese Position wird, wenn auch nicht ganz so explizit, ebenfalls im Aufsatz *Anal Terror* formuliert, in dem Preciado (2015, 138) »anal politics« als »counter-biopolitics« bezeichnet. Hocquenghems *Homosexual Desire* begreift Preciado (ebd.) dabei als »an instruction manual to render functional an anti-systemic orifice installed in each and every body: the ANUS.« Gleichzeitig erfolgt eine Erweiterung des Körperbegriffs, der nicht mehr nur den menschlichen/weiblichen/männlichen/rassifizierten Körper umfasst, sondern den Körper als »relational, vulnerable platform, socially and historically constructed, whose

limits are constantly redefined« (ebd.) denkt. Preciados (2003, 14) Anliegen umfasst dabei mit dem erweiterten Körperbegriff auch »die Sex- und Genderverhältnisse, die zwischen Körpern und Maschinen entstanden sind.« Kontra-Sexualität realisiere sich über die von Preciado thematisierten, ausschließlich nicht-prokreativen Sexpraktiken,[33] mittels derer eine Herstellung von Körpern, die außerhalb der heteronormativen, naturalisierten Differenz binärer Geschlechterrollen sowie Begehrensstrukturen stehen, erfolgen könne (vgl. ebd., 11, 36–49). Im Zentrum kontrasexueller Praktiken steht dabei notwendigerweise ein Verständnis von »Sexualität als Technologie«, das

> »die unterschiedlichen Elemente des Systems Sex/Gender – also ›Mann‹, ›Frau‹, ›homosexuell‹, ›heterosexuell‹, ›transsexuell‹ ebenso wie deren Praktiken und sexuellen Identitäten – als Maschinen, Produkte, Werkzeug, Apparate, Gadgets, Prothesen, Netze, Anwendungen, Programme, Verbindungen, Energie- und Informationsströme, Unterbrechungen und Unterbrecher, Schlüssel, Zirkulationsgesetze, Grenzen, Zwänge, Designs, Logiken, Ausstattungen, Formate, Unfälle, Abfälle, Mechanismen, Gebrauchsweisen, Umwidmungen …« (ebd., 11)

denkbar macht. Der Anus als Lustzentrum wird dabei »das transitorische Zentrum einer Arbeit kontrasexueller Dekonstruktion«, da er durch seine Unbrauchbarkeit für prokreativen Sex »außerhalb der durch die sexuelle Differenz erzwungenen anatomischen Grenzen liegt« und in ihm »die Rollen und die Register als universal umkehrbar erscheinen« (ebd., 18–19): Unabhängig von Sex- und Genderkonfigurationen haben alle Körper einen penetrierbaren Anus, und können alle Körper penetrieren. Der Anus könne damit als eine Art Gleichmacher der Körper begriffen werden, über den heteronormative Beschreibungs- und Herstellungsweisen derselben dekonstruiert werden können: Er »konstituiert einen Raum technologischer Arbeit; er ist eine Fabrik der Wiederherstellung des kontrasexuellen Körpers.« (Ebd., 19)

Bioports und Buttplugs

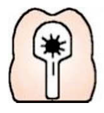
An dieser Stelle soll mit Preciado erneut ein Blick auf die technische Funktionsweise von *Back Orifice* geworfen werden, um das Programm mit dem Konzept der Kontra-Sexualität zu lesen. *Back Orifice* besteht aus zwei Komponenten:

33 Einige Praktiken listet Preciado im *Kontrasexuellen Manifest* in Form von Handlungsanweisungen auf, die strukturell an Fluxus-Scores erinnern.

Einem Server, der auf dem Ziel-PC installiert werden muss, und einem Programm, das auf dem PC installiert sein muss, von dem aus der Ziel-PC gesteuert werden soll. Ist der *Back Orifice*-Server einmal auf einem Computer mit *Microsoft Windows 95* installiert, kann von einem zweiten Computer aus eine direkte Verbindung aufgenommen und der erste Computer komplett ferngesteuert werden, und das mit mehr Benutzerrechten als eingeloggte User_innen haben, die direkt vor dem Zielcomputer sitzen – dies ist der bereits bekannte *privileged state*, den Thomas und Francillon als elementaren Teil einer funktionierenden Backdoor beschrieben haben. Von dieser Position aus können Hacker_innen beispielsweise Dialogfenster erscheinen lassen, die einen von ihnen geschriebenen Text beinhalten, oder aber Tastatureingaben mitschneiden oder den Speicher des Zielcomputers auslesen, um hier nur einige Anwendungsmöglichkeiten der Software zu nennen (vgl. Cult of the Dead Cow 1998a). *Back Orifice* lässt sich durch seine geringe Größe als Payload in anderer, unauffälliger Software verstecken (vgl. Little 1998), die dann als Trojaner fungiert, und wurde so durch Softwaretausch, also Software EXchange – im Jargon File mit dem Akronym »SEX« (The Jargon File o.J.c) abgekürzt – zwischen Freund_innen, Bekannten oder über das Usenet und das Internet verbreitet, beispielsweise über öffentlich zugängliche FTP-Server, sogenannte *public directories*, und, um hier ›im Jargon‹ zu bleiben: »*pubic directories*« (The Jargon File o.J.d). Um den eigenen PC vor *Back Orifice* zu schützen, wurden gemeinhin alle Tipps genannt, die auch schon aus den Praktiken zur Prävention vor Computerviren bekannt sind – empfohlen wurde, sich ein rudimentäres Wissen über die Funktionsweise von Computersystemen anzueignen, sowie keine Programme aus unbekannten und/oder ggf. nicht vertrauenswürdigen Quellen zu installieren (Little 1999), also die komplette Bandbreite dessen, was unter *Personal Systems Hygiene* und *Safe Hex* verhandelt wird. Kam es trotz aller Vorsichtsmaßnahmen dennoch zu einer Installation von *Back Orifice*, so wurde der Server bei jedem Neustart des befallenen Computers automatisch gestartet und ausgeführt. Es ist nicht leicht, *Back Orifice* zu bemerken und zu schließen, da es nicht in der Liste der laufenden Prozesse auftaucht. Daher ist es zunächst auch schwierig zu bestimmen, ob auf einem Computer *Back Orifice* installiert ist oder nicht – Thomas und Francillon folgend weist also die *EFSM* (wenigstens auf den ersten Blick) keine Spuren der Backdoor auf. Ein Hinweis kann aber in den Netzwerkverbindungen erkennbar sein: Um die Fernsteuerung eines Computers zu ermöglichen, etabliert *Back Orifice* eine verschlüsselte Verbindung zu dem Computer eines_einer Hacker_in, von dem aus es gesteuert werden soll, indem es

Ports des Zielcomputers ›öffnet‹ und auf ihnen ›lauscht‹.[34] ›Lauscht‹ ein Programm auf einem Port, so bedeutet dies, dass es über den betreffenden geöffneten Port Daten empfangen kann – im Fall von *Back Orifice* wird der Computer dadurch fernsteuerbar. Preciados (2015, 164) Beschreibung des Anus als »bioport«, der nicht nur ein Symbol sei, sondern »an insertion port through which a body is open and exposed to another or others«, sowie die Fernsteuerbarkeit des Zielcomputers nach der Öffnung eines Ports, den ich hier analog zum Anus lese, greift die bereits besprochenen Dynamiken der Passivierung des_der anal Penetrierten auf. Auch das Logo von *Back Orifice* ist in diesem Zusammenhang bemerkenswert: Es nimmt die Form eines Schlüssels auf, dessen Reite gleichzeitig der weit geöffnete Anus eines minimalistisch dargestellten, weißen Hinterns mit Beinansatz ist. Es sind keine Geschlechtsmerkmale erkennbar, und die Figur des Schlüssels taucht erneut als stilisiertes O im Schriftzug *Back Orifice* auf, der rechts von dem Hintern angeordnet ist, und weist so ein zweites Mal auf die Öffnung, das Loch, den geöffneten (Bio-)Port, den Anus hin.

Back Orifice-Logo




Quelle: https://adesinio.tripod.com/Multimedia/Back_orifice_logo.gif&sp=d370 [16.12.2018, Link mittlerweile inaktiv].

34 Ports regeln – vereinfacht gesagt – die verschiedenen Ebenen, auf denen eine Verbindung zweier Computer miteinander zustande kommen kann, indem sie Verbindungen mit unterschiedlichen Transportprotokollen wie TCP, UDP oder Telnet unterschiedliche Nummern zuweisen, etwa wie bei einem Adresszusatz. Ports stellen also die Endpunkte vernetzter Kommunikation dar, die Verbindung zwischen ihnen etabliert den Trans-Port von Datenpaketen. Im Englischen (und teilweise auch im Deutschen) ist der Begriff mehrdeutig und bezeichnet sowohl die bereits beschriebenen Verbindungen, als auch einen Hafen, sowie Anschlussstellen technischer Geräte, wie beispielsweise beim USB-Port, oder Anschlussstellen menschlicher Körper, wie sie beispielsweise zur Verabreichung von Chemotherapie verwendet werden.

Auch die zahlreichen Wortspiele, die *Back Orifice* umgeben, arbeiten an den Verquickungen mit – die Plug-Ins, also installierbare Erweiterungen, die nicht standardmäßig zur Software gehören, werden als »Buttplugs« bezeichnet (Cult of the Dead Cow 1998b) – und remediatisieren so das Motiv des *Plug-Ins*. Die ›Buttplugs‹ haben sprechende Namen wie beispielsweise *ButtSniffer* (ein *packet sniffer)*, oder *Butt Trumpet* (versendet heimlich die IP-Adresse des Computers, auf dem der BO-Server installiert ist, an eine einstellbare E-Mail-Adresse, vgl. ebd.). Die Namen der Entwickler_innen *DilDog* und *Sir Dystic*, sowie ein weiteres Plug-In mit dem Namen *Silk Rope* (vgl. ebd.) spielen auf Dildos sowie S/M-Praktiken an. Letztere betrachtet Preciado (2003, 19) als Vorbild für Kontra-Sexualität, da sie in den oft mit ihnen einhergehenden expliziten Verträgen auch die impliziten Verträge der heteronormativen Gesellschaftsordnung sichtbar machten. Auch der von Preciado formulierte kontrasexuelle Vertrag ist am Vorbild von S/M-Verträgen orientiert. Das unter dem Begriff Kontra-Sexualität formulierte Programm zur Verwischung und Auslöschung von Geschlechterdifferenzen durch die Aufwertung analer Penetration legt Preciado (2015, 164) zufolge die Gleichheit heterosexuell-männlich kodierter Körper mit anderen Körpern offen, und »dissolves the opposition between hetero and homosexual, between active and passive, penetrator and penetrated. It displaces sexuality from the penetrating penis to the receptive anus, thus erasing the segregative lines of gender, sex, and sexuality.«

Es wird nicht bei der Passivierung *eines* Computers (und den dazugehörigen User_innen) durch *einen* anderen (und den dazugehörigen User_innen) bleiben. Der kontrasexuelle Vertrag gilt für menschliche Körper, und für maschinische fast umso mehr: Obgleich sich die Hardwarekomponenten von Computern stark unterschieden können, so werden diese Differenzen durch die auf ihnen laufende Software gewissermaßen überschrieben, und die jeweiligen Geräte so aneinander angeglichen, dass sie miteinander kommunizieren können. Dennoch sind diese technischen Zusammenhänge, wie gezeigt werden konnte, informiert von Geschlechterdifferenzen biologischer Körper. Wenn Preciado bemerkt, Sex sei eine »Technologie heterosozialer Herrschaft, die den Körper auf erogene Zonen reduziert« (Preciado 2003, 14) und die Geschlechterdifferenz konsequent als »Hetero-Partionierung des Körpers« (ebd., 15) liest – beim vorliegenden Beispiel ließe sich vielleicht treffender von der Hetero-*Partitionierung* des (maschinischen) Körpers sprechen – dann liegt ein transgressives Potential in Backdoors. Diese können, bewusst implementiert, »electronic information exchange as electrifying heterosexual intercourse« (Chun 2006, 12) denaturalisieren, sowie neue Arten

von Verbindungen offenbaren, die nicht der intendierten Logik der Maschine entsprechen, die auf reibungslose Funktionalität und Effizienz ausgelegt ist.

Der Anus, und damit im vorliegenden Fall die Backdoor, kann Preciado folgend als Gleichmacher begriffen werden: Wie anhand der bisher geschilderten Fallbeispiele deutlich geworden ist, kann jedes System eine Backdoor haben. Hat die heteronormative Lesart und Konstruktion von Computern und Computernetzwerken auch geschichtlich konkrete Hardware-Dispositive informiert, wie Wendy Chuns Beispiel der Werbekampagne eines brasilianischen Internetanbieters mit verschiedenen ›männlichen‹ und ›weiblichen‹ Steckern verdeutlicht (vgl. ebd., 12–14), so ist die Backdoor als Anus als Ort der Verwischung dieser sexuellen Differenz gerade in Bezug auf zunehmend ubiquitär werdende, vernetzte digitale Systeme spannend: Alles kann eine Backdoor haben, auch Systeme, die nicht physisch mittels eines Datenträgers oder Kabels, also mit einer Steckverbindung penetriert werden können. »The anal machine rises up before the heterosexual machine«, schreibt Preciado (2015, 165) – aber wie eine solche Maschine genau aussehen könnte, ist (noch) unklar.

Nachgedanken

Die Umdeutungen von *Back Orifice* mit Bersani und Preciado sind aufgrund der Vielgestaltigkeit von Backdoors nicht beliebig auf andere Backdoors übertragbar. Dennoch bieten sie eine Möglichkeit, anders über Sicherheit vernetzter Computer nachzudenken: Entweder könnte, wie mit Bersani herausgearbeitet, eine Lust an der Unsicherheit entwickelt werden, die gleichermaßen ein befreiendes Moment hat, da sie Nutzer_innen von der Steigerungslogik der Herstellung von Sicherheit enthebt. Oder, wie mit Preciado aufgezeigt wurde, eine Denaturalisierung der heteronormativen Diskursivierung von Computerhardware und Software, die vielleicht zu neuen Formen von *Computation* führen könnte. Sowohl mit Bersani als auch mit Preciado lässt sich die höchst spekulative, aber dennoch spannende Frage stellen, ob IT-Sicherheit anders gedacht werden könnte als bisher. Dieser Frage wird im folgenden Kapitel anhand des noch jungen QueerOS/*Queer Computation*-Diskurses nachgegangen.

5. Für einen queeren Sicherheitsbegriff

Die vorliegende Untersuchung hat in den vorangegangenen Kapiteln anhand wissensgeschichtlicher sowie diskursanalytischer Betrachtungen von Kryptologie und IT-Sicherheit den beiden Bereichen zugrunde liegenden negativen Sicherheitsbegriff herausgearbeitet, der im Verlauf ihrer jeweiligen Geschichte trotz technischer Neuerungen konstant geblieben ist. Anschließend an die im vorigen Kapitel durchgeführten Umdeutungen des homophoben Motivs von IT-Sicherheit anhand der *Back Orifice*-Backdoor wird allerdings eine mögliche Öffnung dieses Diskurses hin zu einem anderen Sicherheitsbegriff erkennbar. Dieses Kapitel versucht sich daher an der Möglichkeit, einen anderen Sicherheitsbegriff für die IT-Sicherheit in Stellung zu bringen. Mit Daniel Loick (2021) schlägt dieses Kapitel einen queeren Sicherheitsbegriff vor, und fragt danach, ob und wie sich dieser für die IT-Sicherheit produktiv denken lässt. Diese Frage wird im Zusammenhang mit dem *QueerOS/Queer Computation*-Diskurs bearbeitet, der sich in den letzten Jahren durch einige Publikationen, die *Computation*, also wie Computer funktionieren und wie sie genutzt werden, und Queerness zusammendenken, gebildet hat. Vor dem Einstieg in diese Diskussion werden zunächst noch mit Eve Kosofsky Sedgwicks (2003) Konzepten des *paranoid* und des *reparative reading* zwei Modi der Wissensproduktion eingeführt, die für eine solche Diskussion notwendig sind, und die Diskurse von IT-Sicherheit und Kryptologie auf ihre Zugehörigkeit zu diesen befragt.[1]

---

1 Teile dieses Kapitels, insbesondere die Diskussion von *paranoid* und *reparative reading* in Hinblick auf mögliche Formen von Sicherheit wurden bereits veröffentlicht (vgl. Shnayien 2022).

5.1 Paranoide und Reparative Praktiken

Die Queertheoretikerin Eve Kosofsky Sedgwick unterscheidet in ihrem Essay *Paranoid Reading and Reparative Reading, or, You're So Paranoid, You Probably Think This Essay Is About You* zwei Arten der Herstellung von Wissen: eine, die strukturelle Ähnlichkeiten zur Paranoia aufweist, und daher von ihr als *paranoid reading* bezeichnet wird, und die ihr gegenüber positionierte Form, die Sedgwick als *reparative reading* bezeichnet. Sedgwick betont die affektive Dimension der Theoriebildung und der Herstellung von Wissen über die Welt, indem sie danach fragt, was es bedeutet, und welche Konsequenzen damit einhergehen (oder auch nicht), Wissen(sproduktion) in einer spezifischen Art zu organisieren. Ihre Überlegungen leitet Sedgwick mit der kurzen Schilderung eines Gesprächs zwischen ihr selbst und der befreundeten ACT UP-Aktivistin Cindy Patton während des ersten Jahrzehnts der AIDS-Krise ein. Sedgwick schildert, wie sie Patton nach ihrer Meinung zu den »sinister rumors about the virus's origin« (ebd., 123) fragt: Wurde das HI-Virus in einem Forschungslabor hergestellt, mit dem Zweck, es als Biowaffe einzusetzen? Patton gibt eine Antwort, die Sedgwick zunächst frustriert zurücklässt:

> »›Any of the early steps in its spread could have been either accidental or deliberate,‹ she said. ›But I just have trouble getting interested in that. I mean, even suppose we were sure of every element of a conspiracy: that the lives of Africans and African Americans are worthless in the eyes of the United States; that gay men and drug users are held cheap where they aren't actively hated; that the military deliberately researches ways to kill noncombatants whom it sees as enemies; that people in power look calmly on the likelihood of catastrophic environmental and population changes. Supposing we were ever so sure of all those things —what would we know then that we don't already know?‹« (Ebd.)

Pattons Antwort ist in der Tat zunächst kontraintuitiv: Würde man nicht annehmen, dass politisches Handeln erfordert, alle Zusammenhänge und Motive, insbesondere die der Akteur_innen, gegen die man sich auflehnt, zu kennen? Würden diese nicht die Sichtweise auf die Situation, in der man sich befindet, das eigene Handeln und die eigene Strategie des Protests informieren? Sedgwick beschreibt, wie sie nach Jahren des Nachdenkens über die erhaltene Antwort feststellt, dass sie diese eben *aufgrund* der in ihr zunächst enthaltenen Trennung von historischen Zusammenhängen und den scheinbar unmittelbar aus ihnen zu folgen habenden Reaktionen als »enabling« (ebd.,

124) empfindet – als einen neuen Möglichkeitshorizont eröffnend: »Patton's comment suggests that for someone to have an unmystified, angry view of large and genuinely systemic oppressions does not intrinsically or necessarily enjoin that person to any specific train of epistemological or narrative consequences.« (Ebd.) Mit dieser Unterbrechung der ansonsten als Kontinuität wahrgenommenen Kette Wissen – Fühlen – Handeln wird die Frage danach, ob ein Verdacht wahr ist oder nicht, nicht mehr zur alles bestimmenden Frage; kann man sich von der Notwendigkeit, einen Verdacht verifizieren oder falsifizieren zu müssen, lösen, und kann, wie Sedgwick (ebd., Herv. i.O.) schreibt, stattdessen einen Ebenenwechsel hin zu den übergeordneten Fragen vollziehen: »What does knowledge *do* – the pursuit of it, the having and exposing of it, the receiving again of knowledge of what one already knows? *How*, in short, is knowledge performative, and how best does one move among its causes and effects?« Während Sedgwick die Kenntnis um die Performativität von Wissen sogleich als banal relativiert, verweist sie auf eine Verschiebung, die sich für ihr Nachdenken als spannender erwiesen habe: Die von Paul Ricoeur beschriebene *Hermeneutik des Verdachts*, und damit die ›Entzauberungsgesten‹ Marx', Nietzsches und Freuds, nach der sich stets *hinter* einem gegebenen Ding die *eigentliche Wahrheit* desselben befinde, die aufgedeckt werden müsse, hat sich in die *Critical Theory* verschoben, bis dieser Modus der Kritik synonym mit dem Üben von Kritik selbst wurde. Sedgwick (ebd., 125) folgert: »Not surprisingly, the methodological centrality of such suspicion to current critical practice has involved a concomitant privileging of the concept of paranoia.« In einer Welt voller offensichtlich zu Tage liegender systemischer Unterdrückung, so schreibt Sedgwick (ebd., 126) weiter, »to theorize out of anything *but* a paranoid critical stance has come to seem naive, pious, or complaisant.« Dabei ist es Sedgwick (ebd., 128–129) wichtig, festzuhalten, dass das Praktizieren von reparativen Formen der Wissensproduktion nicht bedeutet, die Realität zu verleugnen oder Unterdrückung nicht anerkennen zu wollen, sowie dass sich paranoide und reparative Praktiken der Wissensproduktion durchaus abwechseln oder ergänzen können. Sich gegen einen klinisch-pathologisierenden Gebrauch des Wortes Paranoia wendend, kommt es Sedgwick eher darauf an, Paranoia auf seine strukturelle Funktionsweise zu befragen, und diese nicht sofort als zu Verwerfendes oder zu Therapierendes zu markieren:

> »I myself have no wish to return to the use of ›paranoid‹ as a pathologizing diagnosis, but it seems to me a great loss when paranoid inquiry comes to seem entirely coextensive with critical theoretical inquiry rather than being

> viewed as one kind of cognitive/affective theoretical practice among other, alternative kinds.« (Ebd., 126)

Diese Sichtweise erlaubt Sedgwick eine Analyse der Verschiebung von Paranoia als Wissensobjekt anti-homophober Theoriebildung, wie etwa bei Hocquenghem, hin zu Paranoia als Methode. Diese Verschiebung sieht sie in der Funktionsweise von Paranoia begründet: Paranoia sei ansteckend, würde symmetrische Epistemologien hervorbringen (vgl. ebd.), Verdacht gegen (Hinter-)List ins Feld führen und umgekehrt, frei nach dem Motto: »it takes one to know one« (ebd., 127). Das Wissen darum, in einer Welt zu leben, in der systemische Unterdrückung an der Tagesordnung ist, führe dennoch, wie Sedgwick betont, nicht automatisch dazu, Ereignisse paranoid strukturiert narrativieren zu müssen, und ziehe auch nicht zwangsläufig eine bestimmte Haltung oder bestimmte Handlungsoptionen nach sich (vgl. ebd.), kurzum: das Wissen um systemische Unterdrückung habe keine deterministischen Auswirkungen auf zukünftiges Handeln. Paranoia als Methode zu hinterfragen, erlaubt es Sedgwick, Paranoia als Standardmethode der *Critical Theory* vom Thron zu stoßen und als eine mögliche Herangehensweise unter vielen zu markieren: »[P]aranoid practices«, schreibt sie, »represent *a* way, among other ways, of seeking, finding, and organizing knowledge. Paranoia knows some things well and others poorly.« (Ebd., 130, Herv. i.O.) Angesichts der AIDS-Krise, zu deren Zeit sich auch das den Text eröffnende Gespräch mit der befreundeten Aktivistin Patton zugetragen hat, und die Sedgwicks Theoriebildung hier zugrunde liegt, lässt sich die von ihr vorgenommene Unterscheidung von paranoiden und reparativen Praktiken als eine Strategie verstehen. Eine Strategie, die »enabling« (ebd., 124) ist, da ihr Einsatz darauf basiert, in dieser Welt nicht bloß zu überleben, sondern *gut* zu leben,[2] ohne im Spiel des paranoid-reaktiven Antizipierens des Schlimmstmöglichen gefangen zu sein, ohne immer schon von der Welt in eine scheinbar ausweglose Epistemologie des Sterben-Lassens und Umgebracht-Werdens verstrickt worden zu sein.[3] Dabei geht es Sedgwick nicht darum, der reparativen Position mehr Wahrheit

---

2 Die gewählte Formulierung, *gut* zu leben, bezieht sich an dieser Stelle explizit nicht auf die Fantasie des *guten Lebens*, die Lauren Berlant (2011) in *Cruel Optimism* bespricht.

3 Hannah McCann und Whitney Monaghan (2019, 146) weisen darauf hin, dass Sedgwick außerdem bemerkt, dass ihre eigene Kritik, die sie in ihren vorherigen Werken geübt hat, radikaler hätte sein können, wenn sie reparativ geübt worden wäre.

zuzusprechen als der paranoiden, sondern eher um die verschiedenen Konsequenzen, die sich aus den unterschiedlichen Positionierungen ergeben können. Eine Form der Wissensproduktion zu wählen, die nicht paranoid, sondern reparativ ist, zieht andere Kreise, entwirft andere Narrative, und damit verändern sich auch die wahrgenommenen Möglichkeiten für das eigene Handeln, auch, wenn diese, wie bereits angedeutet, nicht deterministisch sind. Es lässt sich ein Bewusstsein dafür entwickeln, dass auch eine paranoid strukturierte Wissensproduktion nicht bedeutet, an diese Form der Wissensproduktion gebunden zu bleiben: Die Position kann gewechselt werden.

5.1.1 Paranoide Praktiken in IT-Sicherheit und Kryptologie

Bisher ist nicht genauer ausgeführt worden, was Paranoia als Methode der Wissensproduktion eigentlich kennzeichnet. Sedgwick macht in ihrem Aufsatz fünf Kriterien aus, anhand derer sie im Verlauf ihres Texts diskutiert, was paranoide Praktiken sind, aber auch, wo in der *Critical Theory* oder der psychoanalytischen Theoriebildung sie diese beobachtet. Dieser Struktur folgt auch das vorliegende Unterkapitel, wenn auch anhand eines anderen Korpus: Basierend auf Sedgwicks Definition paranoider Praktiken als Form der Wissensproduktion wird hier anhand verschiedener Fallbeispiele aufgezeigt, dass Kryptologie und IT-Sicherheit als wissenschaftliche Disziplinen sowohl was die Forschungsdesiderate als auch Techniken, Rhetoriken und Veröffentlichungen angeht, mittels paranoider Praktiken Wissen generieren. Die folgenden Abschnitte orientieren sich daher an den von Sedgwick definierten Merkmalen paranoider Praktiken der Wissensproduktion[4] und diskutieren diese anhand ausgewählter Beispiele aus IT-Sicherheit und Kryptologie, von denen manche ausführlicher behandelt werden, und bei manchen nur kurz auf bereits erfolgte Ausführungen verwiesen wird, was noch einmal als ein kurzer Überblick über die bisherigen Teile dieser Untersuchung dient. Auf reparative Praktiken der Wissensproduktion wird im Anschluss genauer eingegangen.

4 Sedgwick unterteilt ihre Ausführungen zu paranoiden Praktiken in fünf Abschnitte. Die folgenden Ausführungen ziehen zwei dieser Punkte zusammen, daher erfolgt die Diskussion hier in vier Unterkapiteln.

»Paranoia is anticipatory«

»*There must be no bad surprises,*« schreibt Sedgwick (2003, 130, Herv. i.O.), sei der vorderste Imperativ paranoid strukturierter Wissensproduktion. Das Verhindern jeglicher Überraschungen, guter oder schlechter (aber vor allem schlechter) Natur, sei die Grundlage des intimen Verhältnisses von paranoiden Praktiken und Wissen im allgemeinen, und kreiere eine komplexe zeitliche Relation des Wissens zum wissenden Subjekt, in der die unbedingte Ausrichtung auf die Zukunft von der um ihrer Willen zu vermeidenden möglichen Vergangenheit informiert ist: Da es keine bösen Überraschungen geben dürfe, und da bereits die Möglichkeit einer bösen Überraschung eine solche sei, müsse Paranoia auch die schlechten Nachrichten immer schon gewusst haben (vgl. ebd., 130). Die Bewegung nach vorne, um von dort einen Blick zurückzuwerfen, gilt auch für die Relation von Kryptographie und Kryptanalyse, den beiden Teilgebieten der Kryptologie. Befasst sich Kryptographie mit der Verschlüsselung von Nachrichten, so kümmert sich Kryptanalyse um das Brechen von Verschlüsselung auf einem unvorhergesehenen Weg. Nun ließe sich einwenden, dass es keine Kryptanalyse geben könne ohne Kryptographie, denn was würde diese denn entschlüsseln wollen? »But in the real world«, bemerkt David Kahn (1967, 753),

> »the cryptanalyst – or more accurately the potential cryptanalyst – comes first. What need for cryptography if no one would eavesdrop? Why build forts if no one would attack? Thus the assumption that someone will attempt a cryptanalysis, no matter how tentatively or incompetently, engenders cryptography.«

Kryptographie ist also schon immer auf ihren angenommenen Angriff hin ausgerichtet – laut Kahn existiert sie, um einen möglichen Angriff auf sie zu verhindern. Diese stets auf die möglichen Zukünfte gerichtete Zeitlichkeit findet sich auch im Essay *Why Cryptography Is Harder Than It Looks* von Bruce Schneier. Erstmals 1997 im Journal *Information Security Bulletin* erschienen, ist der Beitrag heute auf Schneiers Blog nachzulesen, und wirkt, abgesehen von einigen einleitenden Bemerkungen, wie ein tagesaktueller Essay.[5] Schneier erläutert, warum gute Kryptographie den Kern eines jeden sicheren IT-Systems bil-

---

5 Man würde zwar vermuten, dass ein Beitrag aus der IT-Sicherheit eine – gemessen an dem Tempo technischer Innovation und dem daher schnelllebigen Feld – eher geringe Halbwertszeit haben sollte, doch da der Beitrag sich auf die Prinzipien der Kryptographie bezieht und weniger auf konkrete Verfahren, erscheint er vergleichsweise zeitlos.

det, und zählt anhand verschiedener Faktoren auf, warum es schwerer sei als es aussehe, ein sicheres System herzustellen. Er führt aus, dass mögliche Sicherheitslücken eines digitalen Systems nicht bloß kryptographischer Natur sein können, sondern auch die softwareseitige Implementierung guter kryptographischer Verfahren betreffen können, die Usability eines Systems (und dadurch den korrekten Einsatz der Sicherheitsmechanismen[6]) oder die Modellbildung selbst. Im Schlussplädoyer schreibt Schneier (1997, Herv. MS):

> »History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. *It's always better to assume the worst*. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did.«

Stets vom schlechtestmöglichen Szenario auszugehen, sollte also der Modellbildung zugrunde liegen, nach der ein Verfahren zur Herstellung von Sicherheit auf seine Leistung beurteilt wird. Die Sicherheitsleistung, und damit das Verhältnis von Verschlüsselung zu Entschlüsselung, sei schon immer von Zeit als alles bestimmendem Faktor geprägt gewesen, wie David Kahn (1967, 753) ausführt, »because all practical matters involving mortal men connect eventually with that one inexorable, irreversible, irretrievable factor.« Der Wettlauf um die Zeit verändert sich jedoch mit den Medien, in denen er ausgetragen wird, und den Zeitlichkeiten, in denen diese operieren und die sie herstellen. Kryptologie entwickelte sich Kahn (ebd., 72) zufolge in den ersten 3000 Jahren ihrer Existenz kaum, und wenn, dann nicht linear. Bestehendes Wissen ging mit den Zivilisationen, die es hervorgebracht hatten, unter, anderes wiederum wurde in Schriften erhalten, von wo aus es weiterentwickelt werden konnte. Doch erst mit der Renaissance westlicher Gesellschaften, so führt Kahn (ebd., 72–73) etwas pathetisch aus, habe die Entwicklung der Kryptologie Fahrt aufgenommen, und sei zu größerer Wichtigkeit gekommen: »The story of cryptology during these years is, in other words, exactly the story of mankind.« An dieser Stelle lässt sich spezifizieren: Sie ist die Geschichte westlicher Gesellschaften und ihrer (schneller werdenden) Medien. Mit der Mechanisierung des Schreibens und dem kommerziellen Erfolg der Schreibmaschine Ende des

6 Ein klassisches Beispiel wäre die Verwendung von »1234« oder einem ähnlich leichten Passwort, da die User_innen mit der Fülle an Passwörtern, die sie sich merken müssen, überfordert sind.

19. Jahrhunderts konnte auch die Verschlüsselung in Form von Chiffriermaschinen automatisiert werden (vgl. Landwehr 2008, 42). Dies war vor allem für militärische Zwecke interessant, denn die ersten Chiffriermaschinen automatisierten Additions- oder Substitutionschiffren und beschleunigten diese um ein Vielfaches, da das Nachschauen in einer Tabelle oder einem im Kreis notierten Alphabet damit entfiel (vgl. ebd.). Die Mechanisierung der Ver- und Entschlüsselung erreichte mit dem Brechen der Enigma während des Zweiten Weltkriegs ihr wohl bekanntestes Diskursereignis, das maßgeblich dazu beitrug, dass heute die Sicherheit eines kryptographischen Systems im Hinblick auf ihre Beweisbarkeit in zwei Kategorien beurteilt wird, die beide in Abhängigkeit zur ihrer Berechenbarkeit durch Computer stehen (vgl. Maurer 2016, 57). Die erste Kategorie heißt *information-theoretically secure*,[7] was bedeutet, dass die Verschlüsselung niemals durch Berechnungen mit einer deterministischen Rechenmaschine gebrochen werden kann. Die zweite, und verbreitetere Kategorie trägt den Namen *computationally secure* und meint, dass die Verschlüsselung zwar theoretisch mittels mathematischer Verfahren berechnet und so gebrochen werden kann, aber diese Berechnung unter den gegebenen Umständen nicht praktikabel ist (vgl. ebd.). Dies bedeutet konkret, dass die gewählte Verschlüsselung zu Brechen ein mathematisches Problem darstellt, das sich nicht in Polynomialzeit auf einer universellen Turingmaschine lösen lässt. Maurer (ebd., 58) weist darauf hin, dass die Informatik mathematische Aussagen über *Computation* treffen möchte, und zu diesem Zweck ein mathematisches Modell von *Computation* notwendig wurde, was durch Alan Turing realisiert wurde. Doch schuf Alan Turing ein mathematisches Modell von *Computation*, wie es Maurer schreibt, oder mechanisierte er die Mathematik, wie es Bettina Heintz (1993) darlegt? Mit Turings Aufsatz *On Computable Numbers, With an application to the Entscheidungsproblem* fielen, wie Heintz (ebd., 71) ausführt, auf theoretischer Ebene erstmals ein formalistisches Verständnis von Mathematik und Mechanizität in eins. Die formalistische Auffassung der Mathematik, die gekennzeichnet ist von einem »radikale[n] Verzicht auf Repräsentation« (ebd., 16), wurde erstmals von David Hilbert im 20. Jahrhundert formuliert, obgleich erste Ansätze des Formalismus bis in die zweite Hälfte des 19. Jahrhunderts zurückreichen (vgl. ebd., 17). »In der formalistischen Mathematik«, fasst Heintz (ebd., 16) zusammen,

7 Der Ausdruck *perfectly secure* kann synonym verwendet werden (vgl. Katz/Lindell 2008, 47), wobei der Begriff *information-theoretically secure* selbsterklärender ist.

»gibt es keinen Verweis mehr auf irgend etwas außerhalb des mathematischen Systems, heiße das nun Anschauung, Evidenz, sinnliche Erfahrung oder Intuition. Die Mathematik erzeugt die Objekte, mit denen sie operiert, und die Regeln, nach denen sie vorgeht, selbst und findet sie nicht irgendwo vor […].«

Formalistische Mathematik begreift Mathematik also als ein in sich geschlossenes, logisches System ohne Bezug auf ein Außen. Innerhalb des Systems lassen sich Behauptungen über das Verhältnis von Elementen zueinander aufstellen, verifizieren oder falsifizieren, kurz: für diese Mathematik stehen eher die Beziehungen zwischen ihren Gegenständen als die Gegenstände selbst im Vordergrund (vgl. ebd., 20). Hilbert war angetreten, den Ansatz von Alfred North Whiteheads und Bertrand Russels *Principia Mathematica* (erschienen zwischen 1910–1913) konsequent weiterzudenken. *Principia Mathematica* sollte die Mathematik von dem befreien, was Douglas Hofstadter (2007, 24) als »Seltsame Schleifen« bezeichnet: Den kleinen Widersprüchen der Selbstbezüglichkeit, die sich in die Mathematik über die Mengenlehre oder die Zahlentheorie eingeschlichen hatten. So versuchten Whitehead und Russel, »die gesamte Mathematik, wohlgemerkt ohne Kontradiktionen (!), aus der Logik abzuleiten« (ebd., 26), was bedeutet, die Mathematik auf solide axiomatische Annahmen zu stellen, und alle getätigten Aussagen aus diesen Axiomen logisch herleiten zu können. Den Beweis der Widerspruchsfreiheit dieser umfassenden Unternehmung blieben sie jedoch schuldig (vgl. ebd.), und an dieser Stelle kommt Hilbert ins Spiel. Hilbert wollte genau diesen Beweis liefern, »daß jeder wahre Satz der Zahlentheorie sich innerhalb des von P.M. [*Principia Mathematica*, MS] abgesteckten Rahmens ableiten läßt« – ein Unterfangen, das Hofstadter (ebd.) ebenfalls als eine Seltsame Schleife bezeichnet, denn »[w]ie kann man seine Beweismethoden auf der Grundlage eben dieser Beweismethoden rechtfertigen? Es ist, als wollte man sich an den eigenen Haaren aus dem Sumpf ziehen.« Hilbert hatte seine Theorie an drei Grunderwartungen ausgerichtet: Er veranschlagte, dass die formalistische Mathematik widerspruchsfrei, vollständig und entscheidbar sei – allerdings ebenfalls, ohne dies bewiesen zu haben (vgl. Heintz 1993, 63). Diese Erwartungen wurden der Reihe nach gedämpft: Zunächst durch Kurt Gödel, der 1931 mit dem sogenannten *Unvollständigkeitsbeweis* darlegte, dass inhaltlich wahre Sätze innerhalb eines gegebenen Systems existieren, die nicht aus diesem ableitbar sind, und dass die Widerspruchsfreiheit eines gegebenen Systems niemals aus diesem selbst heraus bewiesen werden kann, sondern nur mittels

eines übergeordneten Systems (vgl. ebd., 64–65). Gödels *Unvollständigkeitsbeweis* falsifizierte damit auch die Grundannahmen von Whiteheads und Russels *Principia Mathematica* (vgl. Hofstadter 2007, 27). Die Widerlegung des Hilbert'schen Programms wurde von der mathematischen Community mit Erleichterung aufgenommen, denn hätte Hilbert Recht behalten, so wäre die Mathematik grundsätzlich mechanisierbar gewesen und die mathematische Beweisführung damit gänzlich automatisierbar, was in letzter Konsequenz Mathematiker_innen obsolet gemacht hätte (vgl. Heintz 1993, 63–64). Alan Turings 1936 erschienener Aufsatz *On Computable Numbers, With an application to the Entscheidungsproblem* bewies nicht die grundsätzliche Mechanisierbarkeit der Mathematik,[8] wohl aber die grundsätzliche Mechanisierbarkeit eines in sich geschlossenen mathematischen Systems (vgl. ebd., 64). Mit der Turingmaschine, fasst Heintz (ebd.) pointiert zusammen, werden »Formalisierung und Mechanisierung [...] bedeutungsäquivalente Begriffe.« Die Turingmaschine entspricht also einem Algorithmus, und für jede im Turing'schen Sinne berechenbare Funktion gibt es eine Turingmaschine. In seinem Aufsatz führt Turing noch eine weitere Maschine ein, die er als *universelle Maschine* bezeichnet. Diese kann jede beliebige Turingmaschine in sich aufnehmen und berechnen. »Mit seiner Arbeit«, so folgert Heintz (ebd., 10), »hat Turing die formalistische Auffassung der Mathematik zu Ende gedacht und sie gleichzeitig radikalisiert: Jede Operation im Rahmen eines formalen Systems läßt sich im Prinzip auch von einer Turingmaschine ausführen.« Die Turingmaschine ist also eine symbolische Maschine, die, ganz nach der Leitidee der formalistischen Mathematik, mit den Relationen ihrer Gegenstände zueinander befasst ist – genau wie das Verhältnis von Kryptographie und Kryptanalyse, von Ciphertext und Plaintext. Ihre erste physische Realisierung erfuhr sie, als Turing und sein Team in Bletchley Park erste Vorläufer unserer heutigen Computer bauten, um die Verschlüsselung der Enigma zu brechen. So ist die Geschichte der Kryptologie untrennbar mit der Geschichte der Informatik verbunden:

---

8 Turing (1987, 19) weist in der Einleitung zu *On Computable Numbers, With an application to the Entscheidungsproblem* (dt. Übersetzung: *Über Berechenbare Zahlen mit einer Anwendung auf das Entscheidungsproblem*) explizit darauf hin, dass die von ihm konstruierte Maschine nur mit bestimmten Zahlen operieren kann: »In den Abschnitten 9 und 10 liefere ich einige Argumente mit der Absicht zu zeigen, daß die berechenbaren Zahlen alle Zahlen einschließen, die natürlicherweise als berechenbar angesehen werden könnten. Insbesondere zeige ich, daß bestimmte große Zahlenklassen berechenbar sind. [...] Die berechenbaren Zahlen umfassen jedoch nicht alle definierbaren Zahlen, wofür das Beispiel einer definierbaren Zahl, die nicht berechenbar ist, gegeben wird.«

Computer entstanden mit der Mechanisierung von Kryptographie und Kryptanalyse. Turing war es also gelungen, eine Schnittstelle zu schaffen, an der sich die Mechanisierung der Mathematik und ein mathematisches Modell computergestützter Rechenvorgänge trafen. An dieser Intersektion wird auch die erste Konsequenz der neuen Medialität von Kryptologie deutlich: Die Symbiose von Mathematik und Maschine generiert das Spannungsfeld *Zeit(/Geld) vs. Rechenleistung*, in der sich die Kryptologie von da an befindet. So ist Schneiers Appell, man solle stets davon ausgehen, dass Wissenschaft und Technik bald zu Dingen in der Lage sein werden, die zu einem gegebenen Zeitpunkt noch unmöglich seien, vor allem in digital-medialen Kontexten relevant: Die stetige Weiterentwicklung der Technik sowie der Rechenleistung erzeugt eine andauernde Beschleunigung. Und tatsächlich erscheint es möglich, diese schlechtestmögliche Zukunft nicht nur nebulös zu erahnen, sondern sie zu berechnen. Christof Paar und Jan Pelzl (2016, 13–14) führen in *Kryptografie Verständlich* aus, dass eine vollständige Einschätzung technologischen Fortschritts (neue Erfindungen eingeschlossen) zwar unmöglich sei, aber sehr wohl anhand des *Mooreschen Gesetzes* die Beschleunigung bereits existierender Systeme in Relation zu monetären und zeitlichen Ressourcen geschätzt werden könne. Dieses Gesetz beschreibt das exponentielle Wachstum von Rechenleistung: Es besagt, dass sich die Rechenleistung von Computern bei konstant bleibenden Kosten alle 18 Monate verdoppelt.[9] Der Verweis auf das Mooresche Gesetz bringt zum ersten Mal auch explizit monetäre Ressourcen in die Evaluation von Sicherheit mit ein, die sich mit zeitlichen Ressourcen abwechseln müssen. Angelehnt an Paars und Pelzls (ebd., 14) Beispiel lässt sich das Mooresche Gesetz anhand einer fiktiven Akteurin folgendermaßen veranschaulichen: In diesem Augenblick müsste sie Computer im Wert von einer Million Euro besitzen, um eine Verschlüsselung in einem Monat zu brechen. In 18 Monaten müsste sie nur eine halbe Million investieren, da die Computer doppelt so schnell rechnen können. In drei Jahren nur noch eine Viertelmillion, in 15 Jahren nur noch 1000€. Alternativ könnte die fiktive Akteurin in 15 Jahren eine Million Euro aufwenden und die Verschlüsselung in 45 Minuten brechen. Diese Überlegungen sind relevant für die Länge der verwendeten Schlüssel bei Verschlüsselungsverfahren, die nach dem *Kerckhoffs'schen Prinzip*

9 Während sich bereits erste Abweichungen von den Vorhersagen des Mooreschen Gesetzes in den letzten Jahren gezeigt haben, ist unklar, ob, und wann genau es seine Gültigkeit verlieren könnte (vgl. Rotman 2020).

funktionieren. Hier gilt: je länger der verwendete Schlüssel, desto exponentiell länger dauert ein *Brute-Force*-Angriff,[10] mit dem der Schlüssel geknackt werden soll. Cloudanbieter und Bankensysteme verwenden in der Regel 256 Bit lange Schlüssel, was einen Brute-Force-Angriff einige Dekaden kostet, selbst für den Fall, dass Quantencomputer eingesetzt würden (vgl. ebd., 13). Einen solchen antizipierenden Blick beschreibt auch Sedgwick (2003, 131) als Modalität paranoider Praktiken der Wissensproduktion: »No time could be too early for one's having-already-known, for its having-already-been-inevitable, that something bad would happen. And no loss could be too far in the future to need to be preemptively discounted.«

»Paranoia is reflexive and mimetic«

Eingangs wurde bereits kurz erwähnt, dass Sedgwick Paranoia als ansteckend betrachtet, und in der Ansteckung die Herstellung symmetrischer Epistemologien erkennt. Diese Ansteckungen, und vor allem die symmetrischen Epistemologien werden, Sedgwick (2003, 131) zufolge, durch die Eigenschaft von Paranoia, sich reflexiv und mimetisch zu verhalten, hergestellt: »Paranoia seems to require being imitated to be understood, and it, in turn, seems to understand only by imitation.« In Anschluss daran formuliert Sedgwick (ebd., Herv. i.O.) eine Art Motto der paranoiden Form der Wissensproduktion: »Paranoia proposes both *Anything you can do (to me) I can do worse*, and *Anything you can do (to me) I can do first* – to myself.« Bezogen auf Kryptographie und IT-Sicherheit lassen sich in den Bereichen der Modellbildung und bei sogenannten Penetrationstests für diese Aussage konkrete Beispiele finden. In Kapitel 2 wurde bereits ausführlich auf die kryptographische Modellbildung der *Beweisbaren Sicherheit* eingegangen, deren Aufgabe es Jonathan Katz und Yehuda Lindell (2008, 23–24) zufolge sei, die Gegebenheiten der Welt in ein mathematisches Modell derselben zu übersetzen, was schlussendlich dazu führt, ein mathematisches Modell der Welt zu entwerfen – ein Ansatz, der innerhalb der *Beweisbaren Sicherheit* durchaus kritisiert wird (vgl. Koblitz 2007). Kryptographische Modellbildung versucht, Sicherheit *vor* etwas herzustellen, und definiert mittels Reduktionen zu diesem Zweck genau, wovor es sichern soll und kann. Die verwendete Methode des_der antizipierten Angreifer_in bleibt, dem »arbitrary

10 Bei einem Brute-Force-Angriff (dt. etwa: Angriff mit roher Gewalt) werden nacheinander sämtliche Möglichkeiten eines Schlüssels durchprobiert, bis der richtige gefunden wurde. Je nach Komplexität des jeweiligen Passworts kann dies sehr schnell gehen, oder aber mehrere Jahrtausende in Anspruch nehmen.

adversary principle« (Katz/Lindell 2008, 22) folgend, strategisch unbestimmt. Die Modellbildung in der IT-Sicherheit geht, wie Schneier (1997) darlegt, etwas anders vor, da sie mehr Aspekte in die Herstellung von Sicherheit einbeziehen muss als die Kryptographie, wie beispielsweise das User Interface, oder die betrieblichen Abläufe, in die ein Kryptosystem eingebunden werden soll. Schneier (1997) beschreibt die Vorgehensweise kompakt:

> »A good design starts with a threat model: what the system is designed to protect, from whom, and for how long. The threat model must take the entire system into account – not just the data to be protected, but the people who will use the system and how they will use it. What motivates the attackers? Must attacks be prevented, or can they just be detected? If the worst happens and one of the fundamental security assumptions of a system is broken, what kind of disaster recovery is possible? The answers to these questions can't be standardized; they're different for every system.«

Die Vorgehensweise von *Threat Modeling* orientiert sich nicht nur an der von Sedgwick beschriebenen antizipierenden Haltung von Kryptographie und IT-Sicherheit, sondern auch an der Notwendigkeit, durch Imitation zu verstehen: Beim Threat Modeling wird aus der Perspektive der Angreifer_innen gedacht, um auf diese Weise möglicherweise auszunutzende Sicherheitslücken innerhalb des eigenen Systems zu identifizieren (vgl. Shostack 2014). Sind diese Sicherheitslücken einmal identifiziert, können sie präventiv angegangen werden: In seinem Handbuch *Threat Modeling. Designing for Security* weist Adam Shostack (ebd., 12–13) darauf hin, dass als Reaktion auf ein identifiziertes Problem vier Möglichkeiten in Frage kommen: 1.) das Ausnutzen einer Sicherheitslücke könne durch zusätzliche Sicherheitsmaßnahmen erschwert werden, 2.) eine Sicherheitslücke könne komplett geschlossen werden, 3.) das identifizierte Problem könne auf eine andere Entität ausgelagert werden, bspw. auf eine Firma, die entsprechende Dienstleistungen anbietet (es könnte dabei z.B. um die DSGVO-konforme Verwaltung von Kund_innendaten gehen), 4.) das Risiko könne akzeptiert werden. Auf diese Weise erzeugt Threat Modeling symmetrische Wissensbestände und Wissensgeschichten: Designer_innen von (sicheren) Systemen orientieren sich an den von ihnen erwarteten Verhaltensweisen von Hacker_innen, um ihre Systeme genau gegen diese abzusichern. Hacker_innen wiederum orientieren sich an dem von ihnen erwarteten Verhalten von Designer_innen, und versuchen dort anzugreifen, wo sie eine Sicherheitslücke vermuten. Dies ist die Symmetrie, die Sedgwick (2003, 131) beschreibt, wenn sie formuliert: »Paranoia seems to

require being imitated to be understood, and it, in turn, seems to understand only by imitation.«

Auf die Spitze getrieben wird dieses Wissensverhältnis zwischen Hersteller_in und Angreifer_in, bei dem stets zu vermuten ist, dass man sich nicht gründlich genug in die andere Partei hineinversetzt habe, beim sogenannten *Penetrationstest*. Bei diesem Verfahren wird ein_e Dienstleister_in damit beauftragt, die Sicherheit eines Unternehmens durch einen Angriff zu testen, nur für den Fall, dass die bisher hergestellte epistemologische Symmetrie noch nicht symmetrisch genug ist. Das auszuschließende *störende Dritte* soll bei diesem Verfahren ein System wortwörtlich penetrieren: Es soll einen Eingang finden. In einem Praxisleitfaden des Bundesamtes für Sicherheit in der Informationstechnik (BSI 2016) heißt es dazu, der Penetrationstest sei ein

> »erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung festzustellen. Hierzu werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft.«

Es werden zwei Arten von Penetrationstests unterschieden: Blackbox-Tests und Whitebox-Tests.[11] Bei Blackbox-Tests stehen den für den Angriff nur Name und Webadresse des zu prüfenden Unternehmens zur Verfügung, bei Whitebox-Tests steht ebenfalls der zu überprüfende Code zur Verfügung, sowie unter Umständen umfangreichere Informationen zur Organisationsstruktur des zu prüfenden Unternehmens (vgl. ebd., 5). Das BSI (ebd., 5–6) empfiehlt die Durchführung von Whitebox-Tests, da bei Blackbox-Tests sowohl der Aufwand für die Prüfer_innen, als auch die Möglichkeit, unbeabsichtigt Schaden anzurichten, höher sei, sowie unter Umständen Angriffspunkte übersehen werden können: »Es besteht die Gefahr, dass im Rahmen eines Blackbox-Tests Szenarien wie der Angriff eines informierten Innentäters nicht berücksichtigt werden.« Penetrationstests lassen sich damit als das von Sedgwick (2003, 131) zusammengefasste Motto der paranoiden Form der Wissensproduktion verstehen: »*Anything you can do (to me) I can do worse*, and *Anything you can do (to me) I can do first* – to myself.« Auf diese Art tragen Penetrationstests, analog zu Sybille Krämers (2008, 149) Bemerkung,

11 Shostack (2014, 192) differenziert zwischen »black box«- und »glass box«-Tests.

Computerwürmer würden zur *Immunisierung* eines Betriebssystems anregen, zur Immunisierung eines gegebenen Systems bei, nur um dieses weiter in Richtung der von Loick (2021, 271) benannten »Fortifizierungslogik« eines negativen Sicherheitsbegriffs zu führen. Die symmetrische Epistemologie, die mit paranoiden Praktiken der Wissensproduktion einhergeht, führt damit zu einer Verhärtung des Wissens und der Praktiken von Designer_innen und Angreifer_innen, die sich in der bereits dargelegten Steigerungslogik zueinander verhalten. So bleibt immer ein generelles Misstrauen bezüglich der Überprüfbarkeit von Sicherheit, ein Restrisiko, das niemals eingeholt werden kann, wie auch Schneier (1997) bemerkt: »No amount of general beta testing will reveal a security flaw, and there's no test possible that can prove the absence of flaws.« Paranoia findet also stets das heraus, was sie schon weiß (vgl. Sedgwick 2003, 135): Dass ein System unsicher ist. So empfiehlt es sich, weiterhin vom Schlimmsten auszugehen, denn »[i]n a paranoid view, it is much more dangerous […] to be unanticipated than often to be unchallenged.« (Ebd., 133)

»Paranoia is a strong theory of negative affects«

Sedgwick (2003, 136) bestimmt Paranoia weitergehend als eine »strong theory of negative affects«. Um sich diesem Punkt zu nähern, definiert sie zunächst eine *strong theory* mit dem Psychoanalytiker Silvan Tomkins (in ebd., 134) als »capable of accounting for a wide spectrum of phenomena which appear to be very remote, one from the other, and from a common source.« Die zentrale Leistung einer solchen Theorie sei es also, ungenau genug zu sein, um ein großes Feld zu organisieren, was sowohl Vor- als auch Nachteile mit sich brächte. Als Gegenteil der *strong theory* bestimmt Tomkins (in ebd.) die »weak theory«, die »little better than a description of the phenomena which it purports to explain« auf Phänomene begrenzt sei, die bereits als nah beieinander erscheinen. Tomkins (in ebd.) trifft die Unterscheidung von *weak* und *strong theory* im Hinblick auf die von ihm vorgelegte Affekttheorie, zu der er schreibt:

> »A humiliation theory is strong to the extent to which it enables more and more experiences to be accounted for as instances of humiliating experiences on the one hand, or to the extent to which it enables more and more anticipation of such contingencies before they actually happen.«

Eine Affekttheorie ist, so formuliert Sedgwick (ebd., 135, Herv. i.O.), »among other things, a mode of *selective* scanning and amplification«, also eine Art, Ereignisse für sich zu sortieren und zu bewerten. Als »humiliation theory«

kann dementsprechend eine Organisationsform begriffen werden, die auf die Vermeidung von Demütigung/Erniedrigung des Selbst ausgelegt ist. Sedgwick (ebd., 134) folgert aus Tomkins Ausführungen, dass eine solche Theorie paradoxer Weise nicht etwa durch das Vermeiden oder Abmildern von Demütigung oder Erniedrigung an Stärke gewinne, sondern vielmehr dadurch, dass sie ihr Versprechen nicht einlöse. Dies bedeutet, um ein Beispiel aus dem Alltag anzuführen, dass man sich so sehr man möchte auf eine Situation vorbereiten, so viele Eventualitäten mitbedenken, immer vom Schlimmsten ausgehen und sich auf dieses vorbereiten kann – schlussendlich wird doch etwas anderes passieren als das, mit dem man gerechnet hat. Die paranoiden Praktiken, mit denen man versucht, negative Überraschungen zu vermeiden, haben sich als ineffektiv herausgestellt, und die Demütigung verdoppelt sich: Nicht nur ist eine (negative) Überraschung eingetreten, sie ist auch *trotz* der eigenen Vorbereitung eingetreten. Das paradoxe Moment besteht Tomkins und Sedgwick zufolge darin, dass die »humiliation theory« nicht für ihre Ineffektivität verworfen werde, sondern dass sie im Gegenteil ihre Stärke aus dem Scheitern ziehe: Man hätte sich eben noch besser vorbereiten müssen. Diese Logik ist in weiten Teilen der Struktur von IT-Sicherheit, aber auch der Kryptographie erkennbar, beispielsweise in der Steigerungslogik, dem Wettrennen zwischen Sicherheitslücken und Sicherheitsupdates, Computerviren und Antivirensoftware etc.: Ständig werden IT-Sicherheitsmaßnahmen am potenziell schlimmstmöglichen zu vermeidenden Szenario ausgerichtet, um dann in letzter Konsequenz doch nicht zuverlässig zu schützen. Die angebotene Lösung entspricht jedoch nicht einer Veränderung des Sicherheitsbegriffs, sondern einer Verstärkung der Sicherheitsmechanismen, einem Sicherheitspatch, einem Update. Dasselbe gilt für die Modellbildung innerhalb der *Beweisbaren Sicherheit*, die vorzugsweise verbessert wird, anstatt ihre Limitationen anzuerkennen (vgl. Katz/Lindell 2008, 23).

Ein weiterer erwähnenswerter Aspekt von Paranoia als »strong theory of negative affects« ist, dass »only paranoid knowledge […] has so thorough a practice of disavowing its affective motive and force and masquerading as the very stuff of truth.« (Sedgwick 2003, 138) Paranoide Wissensproduktion tarne also ihre Affekte als rationale Wahrheitssuche. Sedgwick führt diesen Punkt anhand der Werke Marcel Prousts aus, hier soll dies anhand eines Aufsatzes aus dem Feld der Kryptographie getan werden. In ihrem Aufsatz *A Riddle Wrapped in an Enigma* gehen die Kryptographen Neal Koblitz und Alfred Menezes (2016) genauer auf ein öffentliches Statement der NSA ein, die sich im August 2015 für die Notwendigkeit der Entwicklung von Post-Quanten-

Kryptographie[12] aussprach. Die NSA war nicht die einzige Institution, die sich ungefähr 20 Jahre nach der Entstehung dieses Forschungsgebietes für eine stärkere Förderung desselben aussprach, und so war zunächst nichts an diesem Statement aufsehenerregend. »However, one passage was puzzling and *unexpected*« (ebd., 34, Herv. MS), bemerken Koblitz und Menezes: Organisationen oder Verkäufer_innen, die noch nicht von RSA-Verschlüsselung auf ECC-Verschlüsselung[13] umgestellt hatten, bräuchten dies nicht zu tun, sondern sollten stattdessen ihr Geld für das Update auf Post-Quanten-Protokolle sparen (vgl. ebd., 35). Aus dieser Aussage erwuchs der Verdacht innerhalb der kryptographischen Community, dass die NSA sich von ECC distanziere (vgl. ebd., 35), was zu weiteren Spekulationen führte. Kurz nach Veröffentlichung des NSA-Statements erschien ein Artikel in der *New York Times*, in dem, basierend auf den Snowden-Enthüllungen, die kleptographische Backdoor in DUAL_EC_DRBG öffentlich gemacht wurde (vgl. ebd., 36), was die Diskussion weiter anheizte. Koblitz und Menezes gehen in ihrem Artikel den innerhalb der kryptographischen Community besprochenen einzelnen Verdachtsmomenten, sowie den Diskussionen über die möglichen Motive der NSA nach, die von der angenommenen Fähigkeit der NSA, RSA, ECC oder sogar Post-Quanten-Kryptographie zu brechen, bis hin zu der Idee reichen, die Distanzierung von ECC sei ein gegen Russland und China gerichtetes Täuschungsmanöver. Die Autoren machen sich über keine dieser Theorien lustig, sondern wägen sorgfältig Für und Wider ab, kommen jedoch am Ende ihres Artikels zu keinem Ergebnis: »We cannot offer a definitive conclusion; the reason for the NSA's pulling back from ECC remains an enigma. Readers are invited to choose from the possible explanations we've given, or come up with their own theories.« (Ebd., 42) Koblitz' und Menezes' Artikel ist insofern bemerkenswert, als er in einem renommierten Journal erschienen ist, und dennoch nichts außer Spekulationen beinhaltet, und sogar zu eigenen, weiteren aufruft – so wird der Versuch der Vermeidung negativer Überraschungen durch antizipierende, reflexive, mimetische Strategien als Wahrheitssuche gekleidet.

---

12 Unter der Bezeichnung Post-Quanten-Kryptographie werden kryptographische Verfahren zusammengefasst, die Angriffen mit einem Quantencomputer standhalten.

13 Das Akronym ECC steht für *elliptic curve cryptography*, also für kryptographische Verfahren, die auf elliptischen Kurven rechnen.

»Paranoia places faith in exposure«

Die letzte Eigenschaft paranoider Praktiken der Wissensproduktion, die Sedgwick bespricht, ist der paranoide Glaube an die Performativität von Wissen. Dazu bemerkt sie:

> »Whatever account it may give of its own motivation, paranoia is characterized by placing, in practice, an extraordinary stress on the efficacy of knowledge per se – knowledge in the form of exposure. […] That a fully initiated listener could still remain indifferent or inimical, or might have no help to offer, is hardly treated as a possibility.« (Sedgwick 2003, 138)

In diesem kurzen Ausschnitt lassen sich zwei Momente festhalten. Der erste ist die Form des Wissens als Aufdeckung, Enthüllung, oder Entlarvung. In all diesen möglichen deutschen Übersetzungen des Wortes *exposure* schwingt nicht nur die Geste der Hermeneutik des Verdachts mit, sondern leise auch die Möglichkeit einer Demütigung. Dieser Zusammenhang ist es, der ein bestimmtes Wissen an eine Handlung bindet, respektive die Möglichkeit eines Indifferent-Bleibens angesichts des erworbenen Wissens für unwahrscheinlich erachtet. Sedgwick (ebd.) bemerkt außerdem: »Maybe that's why paranoid knowing is so inescapably narrative.« Diese Struktur mitsamt ihrem Hang zum Erzählen von Geschichten lässt sich vor allem anhand von Whistleblowing beobachten. So sagte beispielsweise der NSA-Whistleblower Edward Snowden über seine Beweggründe, die Öffentlichkeit über die Praktiken der NSA zu unterrichten: »My sole motive is to inform the public as to that which is done in their name and that which is done against them.« (Greenwald et al. 2013) In dieser Motivation schwingt allerdings auch Snowdens Glaube an die Wirksamkeit von Wissen in Form einer Enthüllung mit. Dies erklärt sich im Zusammenhang mit Snowdens Statement aus einem Videointerview mit Laura Poitras und Glenn Greenwald, das später Teil des Dokumentarfilmes CITIZENFOUR (USA/GER, R: Laura Poitras) wurde: »The greatest fear that I have regarding the outcome for America of these disclosures is that nothing will change« (Poitras/Greenwald 2013, TC 10:47-10:58). Die Enthüllung ist also unmittelbar an eine zukünftige Handlung gebunden, oder stellt mindestens bereits eine Handlungsaufforderung dar. Ähnlich, wie Sedgwick (2003, 145) paranoide Praktiken der Wissensproduktion auch bei sich selbst erkennt und diese in ihrem Aufsatz adressiert, möchte ich dies an dieser Stelle auch tun. Meinen Artikel *Der rosafarbene Elefant im Raum. Überlegungen zur fehlenden Wut über die NSA-Affäre*, der ein Jahr nach den Snowden-Enthüllungen erschien, und darüber hinaus von dem Ansteckungspotential der paranoiden Position zeugt, empfinde ich heute als

nahezu lehrbuchhaft von paranoiden Praktiken der Wissensproduktion getragen:

> »Zieht man derzeit Bilanz über die NSA-Affäre, die dazugehörige Berichterstattung und die Reaktionen von Politik und Bevölkerung, so muss man feststellen, dass [...] die Reaktionen auf die Enthüllungen zu wünschen übrig lassen. [...] Dabei sollte man meinen, eine solche Einsicht in Geheimdienstpraktiken und die damit verbundene Erkenntnis, flächendeckend überwacht zu werden, würde größere Empörung hervorrufen. Stattdessen lassen sich Gleichmut, ja sogar Resignation ob der ganzen Angelegenheit beobachten.« (Shnayien 2014, 1)

Diese Textstelle folgt der Bemerkung Sedgwicks (2003, 138), dass die Vorstellung, »a fully initiated listener could still remain indifferent or inimical« so weit entfernt erscheint, dass sie nicht einmal als Möglichkeit in Betracht gezogen wurde – die damit einhergehenden negativen Affekte machten sich umso stärker bemerkbar.

5.1.2 Reparative Praktiken

Die bisherigen Kapitel dieses Buchs haben gezeigt, dass sowohl Kryptologie als auch IT-Sicherheit als Disziplinen ein negativer Sicherheitsbegriff zugrunde liegt. Mit Sedgwicks fünf Eigenschaften paranoider Praktiken der Wissensproduktion wurde anhand von Beispielen aus den beiden Disziplinen verdeutlicht, dass diese ihr Wissen mit paranoiden Praktiken generieren: Im Zentrum beider Disziplinen steht der Wunsch nach einer Vermeidung oder Abmilderung negativer Affekte, die mit dem Hack, dem Knacken von Verschlüsselung, mit dem Einbruch des *störenden Dritten* in das als geschlossen und sauber imaginierte System verbunden sind. Vor diesem Hintergrund lässt sich auch der negative Sicherheitsbegriff, der Sicherheit *vor* etwas herstellt, das er antizipieren, verstehen, und basierend auf diesem Verstehen präventiv verhindern muss, als von paranoiden Praktiken der Wissensproduktion gekennzeichnet lesen. Doch Paranoia gründet in IT-Sicherheit und Kryptologie auch auf der Nicht-Einholbarkeit der Welt durch das Modell: Medien und Menschen verhalten sich nicht so, wie die kryptographische Modellbildung oder das *threat modeling* der Informatik es antizipieren. In der stets ineffektiven Vermeidung der negativen Affekte erweist sich der paranoid strukturierte Diskurs als eine (Ab-)Sicherungsstrategie: Ein Hack konnte zwar nicht verhindert werden, dafür war aber wenigstens niemand überrascht. Paranoide Praktiken erweisen

sich damit einerseits über den negativen Sicherheitsbegriff als Strategien der Herstellung von Sicherheit, sowie innerhalb des Diskurses durch ihr Wesen einer »strong theory of negative affects« als Sicherungsstrategien des Diskurses selbst.

An diese Erkenntnisse anschließend stellen sich die Fragen, wie man sich mit reparativen Praktiken und Lesarten der Kryptologie und der IT-Sicherheit nähern kann, ob reparative Praktiken der Wissensproduktion eine Rolle für Kryptologie und IT-Sicherheit spielen könnten, und wenn ja, welche. Dazu muss zuerst bestimmt werden, was reparative Praktiken sind oder sein können. Sedgwick geht in ihrem Aufsatz erstaunlich kurz auf diese ein, und spezifiziert sie nicht in derselben Ausführlichkeit, wie sie paranoide Praktiken behandelt. Heather Love (2010, 237, Herv. i.O.), eine ehemalige Schülerin Sedgwicks, schreibt in ihrem Artikel *Truth and Consequences: On Paranoid Reading and Reparative Reading*, in dem sie ihre Beziehung zu Sedgwick, sowie zu deren Aufsatz reflektiert: »Reparation in the essay is on the side of *multiplicity, surprise, rich divergence, consolation, creativity,* and *love*.« Eine reparative Position, soviel verrät auch Sedgwick (2003, 146), sei offen für Überraschungen, oder empfinde es als realistisch, überrascht zu werden. Reparative Praktiken sind, oder vielmehr die Einnahme einer reparativen Position bei Sedgwick sei, wie Anja Michaelsen (2018, 98) in ihrem Aufsatz *Sedgwick, Butler, Mulvey: Paranoide und reparative Perspektiven in Queer Studies und medienwissenschaftlicher Geschlechterforschung* ausführt, als ein »politisch notwendiger Perspektivwechsel formuliert«, der im Zeichen eines »besseren Verständnisses für die lebensermöglichenden Strategien unterdrückter und marginalisierter Gruppen« stehe. Dies lässt sich vor allem anhand der Sätze erkennen, mit denen Sedgwick (2003, 150–151) ihren Aufsatz schließt:

> »No less acute than a paranoid position, no less realistic, no less attached to a project of survival, and neither less nor more delusional or fantasmatic, the reparative reading position undertakes a different range of affects, ambitions, and risks. What we can best learn from such practices are, perhaps, the many ways selves and communities succeed in extracting sustenance from the objects of a culture – even of a culture whose avowed desire has often been not to sustain them.«

Bezugnehmend auf diese Textstelle weist Michaelsen (2018, 98) darauf hin, dass eine reparative Position durch die Verschiebung des Erkenntnisinteresses von der Funktionsweise struktureller, systemischer Gewalt hin zu den Elementen und Modi, »die eine Existenz unterdrückter und marginalisierter

Subjekte ermöglichen – nicht erst nach Überwindung der bestehenden Gegebenheiten, sondern innerhalb dieser« weder beabsichtige, »die Bedeutung systemischer und systematischer Gewalt zu relativieren noch Identitäten zu re-essenzialisieren.« Dennoch könnte eine paranoide Position ihr ebendies vorwerfen, denn das Einnehmen einer reparativen Position ist, wie Sedgwick formuliert, nicht leicht: Die paranoiden Praktiken leisten Widerstand gegen andere Formen der Wissensproduktion. Paranoides Wissen »systematically disallows any explicit recourse to reparative motives«, was auch dazu führe, dass reparative Vorgehensweisen von einer paranoiden Position aus als unzulässige Formen der Wissensproduktion erscheinen, »both because they are about pleasure (›merely aesthetic‹) and because they are frankly ameliorative (›merely reformist‹).« (Sedgwick 2003, 144) Mit anderen Worten: Die explizit politische Ausrichtung der Wissensproduktion zeichne sich innerhalb eines dominant-paranoiden Diskurses deutlich ab, und werde sogleich als zu politisch (»merely reformist«), zu unaussagekräftig oder irrelevant (»merely aesthetic«) verworfen. Diese Abwehrmechanismen der paranoiden Position gegenüber der reparativen werfen auch die Fragen auf, welche Geste Sedgwicks Aufsatz vollzieht, und wie er gelesen wird: paranoid oder reparativ? Love (2010, 238) weist darauf hin, dass der Aufsatz sich nicht dafür ausspreche, ausschließlich reparative Positionen zu vertreten, und in weiten Teilen selbst paranoid strukturiert sei. Diese Ambivalenz ist jedoch hauptsächlich der reparativen Position zu verdanken: Wenn reparative Lesarten die Möglichkeit für Überraschungen offenhalten, so gilt dies nicht nur für positive, sondern ebenso für negative Überraschungen (vgl. Sedgwick 2003, 146). Damit geht, wie Love (2010, 239) anmerkt, auch einher, dass reparative Praktiken der Wissensproduktion die Tür vor paranoiden Praktiken nicht verschließen. Ihre eigene Lesart von Sedgwicks Aufsatz, bemerkt Love (ebd., 238–239), »vacillates between a schizoid-paranoid mode and a reparative mode. What the essay argues, and what it performs, is the impossibility of choosing between them.« Diese Leseerfahrung kann ich durchaus teilen: Sedgwicks Aufsatz spielt mit seinem eigenen Oszillieren, sowohl in den Modi der Adressierung als auch in den Modi der Bezugnahme auf seine Gegenstände, und hat sich in seiner Bedeutung für mich während des Schreibprozesses mehrfach verändert. Dennoch ist das Wechseln zwischen paranoiden und reparativen Lesarten kein Ausgeliefertsein an den Text, und auch bezogen auf weitere Texte und Gegenstände vielmehr eine Art aktiver Übung, die voller Überraschungen steckt. Das Einüben des Wechsels der Positionen lässt sich selbst als eine reparative Geste beschreiben, denn es ist eine Erfahrung geprägt von »*multiplicity, surprise, rich*

divergence, consolation, creativity, and *love«* (ebd., 237), die neue Perspektiven auf die eigenen Gegenständen ermöglicht, sowie andere Arten, sich zu diesen in Beziehung zu setzen. Sind die Diskurse der IT-Sicherheit und Kryptologie maßgeblich geprägt von paranoiden Praktiken, die zweifelsohne auch das vorliegende Buch *angesteckt* haben, lässt sich an dieser Stelle dennoch mit Michaelsen (2018, 107) resümieren: »Es ist nicht so, dass es keinen Anlass zur Paranoia gäbe. Mit Sedgwick stellt sich jedoch die Frage, ob unsere Energien am sinnvollsten in diesem Projekt des Aufspürens und Entlarvens eingesetzt sind.« Was wäre vor diesem Hintergrund also ein reparatives Projekt, auf das sich die Energien stattdessen fokussieren könnten? Wie ließe sich Sicherheit in Kryptologie und vernetzten Computersystemen reparativ denken? Oder, um Sedgwicks Einsatz mit Heather Love (2010, 236) noch einmal etwas offener zu formulieren: »I am enabled – but to do what?«

5.2 Queere (IT-)Sicherheit?

Als ein Beispiel für reparative Praktiken der Wissensproduktion, die, wie bereits mit Michaelsen (2018, 98) ausgeführt wurde, eine Verschiebung des Erkenntnisinteresses von struktureller, systemischer Gewalt hin zu Praktiken, »die eine Existenz unterdrückter und marginalisierter Subjekte ermöglichen – nicht erst nach Überwindung der bestehenden Gegebenheiten, sondern innerhalb dieser«, lässt sich der *Safe/r Sex*-Diskurs der 1980er Jahre anführen. Auch Daniel Loick (2021, 12) bespricht diesen im Zuge seiner Ausführungen zu einem *queeren Sicherheitsbegriff,* den er in Anlehnung an Christoph Menkes und Juliane Rebentischs Konzept der »ästhetischen Freiheit«, sowie anhand des *Safe/r Sex*-Konzepts entwickelt. Ein queerer Sicherheitsbegriff zeichnet sich Loick (ebd., 13) zufolge »durch die Dekonstruktion der strikten Opposition von Sicherheit und Unsicherheit, durch einen Platz für Negativität im Positiven« aus, mittels derer sich die xenophoben Mechanismen, sowie das Phantasma einer zu erreichenden absoluten Sicherheit des negativen Sicherheitsbegriffs vermeiden ließen. Diese Dekonstruktion der binären Opposition von Sicherheit und Unsicherheit beobachtet Loick (ebd., 13–14) vor allem in den Fürsorge- und Sicherheitspraktiken der AIDS-Aktivist_innen der 1980er Jahre:

> »Der AIDS-Aktivismus bringt die bürgerliche Einteilung in Privatheit und Öffentlichkeit zum Kollabieren, indem sie von vornherein die öffentli-

> che Bedeutung ›privater‹ Handlungen exponiert: Sexuelles Begehren und sexuelle Aktivitäten, die Sorge um und für Partner*innen, Trauer- und Begräbnisrituale hatten einen unmittelbar politischen Charakter, sie stehen zur Mehrheitsgesellschaft in einem konfrontativen oder polemischen Verhältnis. Dementsprechend ging es in der ›AIDS-Krise‹ auch nicht allein um das persönliche, sondern auch um das kollektive Überleben, das heißt um das Überleben einer Form von subalterner Sozialität und Kultur.«

In diesem Kontext weist Loick den Grundannahmen von *Safe/r Sex* besondere Relevanz zu: *Safe/r Sex* richtete sich, wie bereits in Kapitel 3 angerissen, gegen das dominante homophobe Narrativ der 1908er Jahre, HIV/AIDS sei eine Strafe für die Hand in Hand gehenden Sünden Homosexualität und Promiskuität. Loick verweist auf Douglas Crimps Aufsatz *How To Have Promiscuity in an Epidemic*, in dem Crimp (1987a, 253, Herv. i.O.) dieses dominante Narrativ angreift, und formuliert: »*it is our promiscuity that will save us*.« Crimp (ebd., 253) führt aus:

> »We were able to invent safe sex because we have always known that sex is not, in an epidemic or not, limited to penetrative sex. Our promiscuity taught us many things, not only about the pleasures of sex, but about the great multiplicity of those pleasures. It is that psychic preparation, that experimentation, that conscious work on our own sexualities that has allowed many of us to change our sexual behaviors – something that brutal ›behavioral therapies‹ tried unsuccessfully for over a century to force us to do – very quickly and very dramatically.«

Die Besonderheit des queeren Sicherheitsbegriffs, führt Loick (2021, 14–15, Herv. i.O.) basierend auf Crimp aus, bestehe in der Erkenntnis, dass queere Sicherheit nicht davon ausgehe, dass nicht-heteronormativer, nicht mit Reproduktion assoziierter Sex per se sicherer sei, sondern dass sich »Sicherheit nur dadurch her[stellt], *dass man sich der Unsicherheit aussetzt.* Damit wird die Dichotomie von Sicherheit und Risiko dekonstruiert: die Unmöglichkeit von Sicherheit ist zugleich die Bedingung ihrer Möglichkeit.« Ein queerer Sicherheitsbegriff, wie ihn Loick anhand von *Safe/r Sex* definiert, lässt sich darüber hinaus mit Sedgwick und Michaelsen als reparative Praktik einstufen: Er ermöglicht marginalisierten Personen ein Überleben, aber auch ein gutes Leben, *innerhalb* einer gesellschaftlichen Struktur, und nicht erst nach Überwindung derselben. Nicht durch die Versuche der Vermeidung von Negativität, was das Ziel paranoider Praktiken wäre, sondern durch die

Anerkennung von Negativität und Unsicherheit als Teil sowie notwendige Voraussetzung von Sicherheit lässt sich diese herstellen. Mit Loick (ebd., 16) lässt sich anschließen:

> »Die Relevanz des queeren Sicherheitsbegriffs – eines Sicherheitsbegriffs also, der sich bewusst ist, dass Sicherheit sich nur durch die Öffnung gegenüber der Unsicherheit realisieren lässt – ist dabei nicht auf die Frage des Sex beschränkt, sondern betrifft auch andere Themenbereiche.«

Während Loick an dieser Stelle mit einer Diskussion von queerer Sicherheit in Bezug auf *Safe/r Spaces* anschließt, kommt die vorliegende Untersuchung zu der Frage zurück, ob und wie eine reparative Perspektive auf Sicherheit vernetzter Computer geworfen werden kann, und formuliert die Frage neu: (Wie) kann ein queerer Sicherheitsbegriff für die IT-Sicherheit in Stellung gebracht werden?

5.2.1 *Queer OS/Queer Computation*

Aufgrund des Zusammenhangs des queeren Sicherheitsbegriffs mit dem Konzept von *Safe/r Sex*, und damit mit dem aktivistischen HIV/AIDS-Diskurs, sowie der Bestimmung von queerer Sicherheit als reparativer Praktik der Wissensproduktion und der Bezugnahme auf die Welt, soll der Frage nach der Produktivität eines queeren Sicherheitsbegriffs für die IT-Sicherheit in diesem Unterkapitel anhand einer Reihe von Aufsätzen nachgegangen werden, die sich explizit dem Zusammenhang von Queerness und Technik widmen, und sich lose unter den Schlagworten *Queer OS* und *Queer Computation* versammeln lassen. Dazu zählen die seit 2013 erschienenen Artikel Jacob Gabourys, die sich mit queeren Persönlichkeiten der Technikgeschichte befassen, jedoch nicht, um eine Ansammlung von Biografien im Sinne einer personifizierten Technikgeschichte vorzulegen, sondern um erstmals eine queere Genealogie der Computergeschichte zu schreiben (vgl. Gaboury 2013a; 2013b; 2013c; 2013d; 2013e). 2014 veröffentlichte Kara Keeling ihre Gedanken zu *Queer OS*, und zwei Jahre später folgte der korrespondierende Text *QueerOS: A User's Manual* von Fiona Barnett, Zach Blas, Micha Cárdenas, Jacob Gaboury, Jessica Marie Johnson und Margaret Rhee (2016). Wiederum zwei Jahre später folgte Jacob Gabourys (2018) Artikel *Critical Unmaking: Toward a Queer Computation.*[14] Gemein-

---

14 Es ließen sich durchaus noch weitere Texte zu dieser Gruppe zählen, beispielsweise Wendy Chuns (2012) *Race and/as Technology or How to Do Things to Race* oder Tara Mc-

sam ist all diesen Texten der Versuch, *Computation*, also die mathematisch-technischen Strukturen und Materialitäten von Computern, sowie deren Eigenheiten und Nutzungspraktiken mit *Queerness*,[15] den Lebensrealitäten, Philosophien, Utopien und Dystopien queerer Menschen, zusammenzudenken, und auf die Modi ihrer Überschneidungen hin zu befragen. Im Folgenden wird zunächst anhand kritischer Lektüren der drei für das vorliegende Unterkapitel zentralen Texte *Queer OS*, *QueerOS: A User's Manual* und *Critical Unmaking: Toward a Queer Computation* das Verhältnis von Queerness und *Computation* in den jeweiligen Aufsätzen diskutiert, und anschließend Anknüpfungspunkte an Sedgwicks *reparative reading* ausgemacht. Weiterhin werden die gewonnenen Erkenntnisse über den *Queer Computation*-Diskurs im Hinblick auf die zentrale Frage des vorliegenden Kapitels, das Nachdenken über einen queeren Sicherheitsbegriff für die IT-Sicherheit, produktiv gemacht.

Queer OS

Kara Keeling (2014, 152) beginnt ihren Artikel *Queer OS* mit der Feststellung, »[f]rom new media's eccentric temporalities and reliance on reading codes to their relationships to ephemera, publics, viruses, music, and subcultures, new media intersect with queer theories in a variety of ways.« An diesen Intersektionen sei bisher Wissen über »queer cybercultures« hergestellt worden, sowie »explorations of the role of new media in LGBT, and queer people's lives«, und wichtige Erkenntnisse zu »representation of LGBT people in, on, and through new media« (ebd.). Dennoch, bemerkt Keeling, gebe es eine Lücke: Während Arbeiten, die sich mit dem Zusammenhang von *race* und neuen Medien befassen, zwar anschlussfähig seien an Positionen der Queer Theory, so werde dieser Zusammenhang nur selten explizit gemacht. Und auch feministische Analysen von Phänomenen digitaler Kulturen, die von einer umfassenderen Beschäftigung mit Queer Theory profitieren könnten, liefern bisher in Keelings

---

Phersons (2012) *U.S. Operating Systems at Mid-Century. The Intertwining of Race and UNIX*, die an dieser Stelle jedoch ausgenommen werden sollen, da sie sich nicht explizit mit Queerness befassen. Die folgenden Überlegungen konzentrieren sich auf Keeling (2014), Barnett et al. (2016), und Gaboury (2018).

15 *Queer*, das sich mit »verdreht« oder »versaut« oder »merkwürdig« ins Deutsche übersetzen lässt, wurde in den 1980er Jahren als abwertende Bezeichnung für homosexuelle Männer und Frauen gebraucht (vgl. Deuber-Mankowsky 2017b, 12). Nach seiner Umdeutung durch Aktivist_innen wird der Begriff heute von Menschen, deren Geschlechtsidentität und/oder Begehren keinem heteronormativen Modell entsprechen, affirmativ als Selbstbezeichnung gebraucht (vgl. Plötz 2014).

Augen bestenfalls Anschlusspunkte an diese (vgl. ebd., 152–153). In Anbetracht dieser von ihr diagnostizierten Lücke in der Theoriebildung schlägt Keeling (ebd., 153) ein »scholarly political project« vor, das sie »Queer OS« nennt, und »at the interfaces of queer theory, new media studies, and technology studies« situiert. Keeling (ebd.) schreibt dazu ausführlicher:

> »Queer OS would take historical, sociocultural, conceptual phenomena that currently shape our realities in deep and profound ways, such as race, gender, class, citizenship, and ability (to name those among the most active in the United States today), to be mutually constitutive with sexuality and with media and information technologies, thereby making it impossible to think any of them in isolation. It understands queer as naming an orientation toward various and shifting aspects of existing reality and the social norms they govern, such that it makes available pressing questions about, eccentric and/or unexpected relationships in, and possibly alternatives to those social norms.«

Wissenschaftliche Arbeiten, die sich unter dem Begriff Queer OS versammeln ließen, führt Keeling (ebd.) aus, seien bereits im Entstehen begriffen, und werden von ihr im Verlauf ihres Artikels besprochen. Ohne Keelings Schilderungen zu diesen Arbeiten detailliert wiedergeben zu wollen, soll zunächst noch einmal genauer nachgezeichnet werden, welche Implikationen Keelings Queer OS beinhaltet. Wie ist der Begriff Queer OS, also ein Queer *Operating System*, ein queeres *Betriebssystem*, angesichts Keelings Vision zu situieren? Handelt es sich dabei um ein Betriebssystem für Maschinen oder für Gesellschaft, oder beides? Keeling (ebd., 153–154) schließt mit diesem Begriff an den drei Jahre zuvor erschienenen Artikel *U.S. Operating Systems at Mid-Century. The Intertwining of Race and UNIX* von Tara McPherson an, und begreift damit Betriebssysteme nicht als bloß technische Systeme, sondern als ›Betriebssysteme einer höheren Ordnung‹. Spezifisch bezieht sich Keeling auf McPhersons (2012, 22) Formulierung »[…] UNIX is widely understood to embody particular philosophies and cultures of computation, ›operating systems‹ of a larger order […].« Im Verlauf ihres Artikels expliziert McPherson, in welcher Weise mit UNIX als Betriebssystem eine dazugehörige Philosophie verbunden sei, eine Idee davon, wie *Computation* aussehen könnte, und eine Gesellschaft, die diese ermöglicht hat, und in die sie gleichsam zurückwirkt. Diese Übertragungsprozesse zeichnet McPherson sehr sorgsam nach, und achtet darauf, die zwei Wissenskulturen, als die sie die Informatik und die Geisteswissenschaft identifiziert, in ihren Unterschieden genau zu erfassen, aber miteinander in einen Dialog zu

bringen. Eine so strikte Trennung von Informatik/Naturwissenschaften und Geisteswissenschaften, wie sie von C.P. Snow (2012) in *The Two Cultures* vorgenommen, oder auch im Zuge des Sokal Hoax formuliert wurde, bezeichnet McPherson (2012, 33) zwar als Mythos, bemerkt aber weiter:

> »[…] powerful operating systems have surged beneath the surface of what and how we know in the academy for well over half a decade. It would be foolish of us to believe that these operating systems – in this paper best categorized by UNIX and its many close siblings – do not at least partially overdetermine the very critiques we imagine that we are performing today.«

McPhersons *operating systems* sind damit nicht nur im wörtlichen Sinne als informatische Betriebssysteme zu begreifen, sondern auch als die Effekte der Betriebssysteme von Computern, die sich bis hinein in die (geistes-)wissenschaftliche Theoriebildung bemerkbar machen,[16] und damit im metaphorischen Sinne als gesellschaftliche Organisationsstrukturen benannt werden können.

Durch die Übernahme der Formulierung des Betriebssystems höherer Ordnung, das sie mit McPhersons zuvorderst zitierter Bemerkung als gesellschaftliche Organisationsstruktur identifiziert, bringt Keeling *Queer* als eine gesellschaftliche Organisationsstruktur in Stellung: »Queer OS makes this formulation of *queer* function as an operating system along the lines of what Tara McPherson describes as ›operating systems of a larger order‹ than the operating systems that run on our computers.« (Keeling 2014, 153) Darüber hinaus verwendet Keeling *Queer* auch als ein Element eines solchen Ordnungssystems. So schreibt sie weiter: »[…] Queer OS seeks to make *queer* into the logic of ›an operating system of a larger order‹«, und bestimmt *queer* damit als Element eines gesellschaftlichen Ordnungssystems »that unsettles the common senses that secure those presently hegemonic social relations that can be characterized by domination, exploitation, oppression, and other violences.« (Ebd., 154) Das Ziel eines *Queer OS* definiert Keeling (ebd.) im Anschluss als

> »[…] to provide a society-level operating system (and perhaps an operating system that can run on computer hardware) to facilitate and support imaginative, unexpected, and ethical relations between and among living beings

16 Auch McPhersons Text selbst unterliegt den Effekten der Modularisierung, die sie in ihrem Aufsatz zu kritisieren versucht (vgl. McIlwain 2020).

> and the environment, even when they have little, and perhaps nothing, in common.«

Keelings *Queer OS* ist damit eine ambivalente Konstellation: Zum einen ein Betriebssystem höherer Ordnung, womit Keeling in loser Anlehnung an McPherson ein gesellschaftliches Ordnungssystem bezeichnet, zum anderen möglicherweise auch ein informatisches Betriebssystem für Computer. Obgleich die Formulierung eines queeren Betriebssystems auf gesellschaftlicher Ebene durchaus charmant klingt, lässt sich die Idee eines gesellschaftlichen Betriebssystems als eine recht flache Lesart von McPhersons (2012, 22) Verwendung des Begriffs verstehen, die die Betriebssysteme höherer Ordnung bereits bei ihrer ersten Nennung durch Anführungszeichen als uneigentliche Rede markiert. Im Verlauf von McPhersons Artikel sind mit Betriebssystemen in erster Linie informatische Betriebssysteme gemeint, die anhand von UNIX zusammen mit ihren Medieneffekten einer genaueren Betrachtung unterzogen werden. Dabei fokussiert sich McPherson (ebd., 29–31) hauptsächlich auf die Modularisierung von Abläufen innerhalb von Computern, die sie in gesellschaftlichen Wissensbeständen und Sphären gespiegelt sieht, beispielsweise in der Aufteilung des öffentlichen Raumes durch die *racial segregation*-Politik der 1960er Jahre. Ein weiterer Schauplatz, an dem die Logik von Computern auf die Gesellschaft zurückwirke, in der sie entstanden und situiert sei, stellt für McPherson die wissenschaftliche Theoriebildung dar. So charakterisiert sie insbesondere die Filmwissenschaft als gekennzeichnet von weißen Flecken in Bezug auf digitale Kulturen, was sie als (Medien-)Effekte derselben begreift (vgl. ebd., 34–36). Bei Keeling (2014, 154) fallen nicht nur die von McPherson gesetzten Anführungszeichen um das Betriebssystem als Metapher weg, wodurch dieses eigentümlich naturalisiert wird, sondern ereignet sich auch eine in zwei Schritten verlaufende Operationalisierung von *queer* in der Formulierung »Queer OS seeks to make *queer* into the logic of ›an operating system of a larger order‹«, die mit Deuber-Mankowsky (2017a, 160, 165) als ein »ontologisches Debakel«, und damit als eine konzeptuelle Verflachung von *queer* begriffen werden kann: Der erste Schritt ist die Konzeptualisierung von Gesellschaft als Betriebssystem. Durch diese Übertragung informatischen Vokabulars auf die Gesellschaft erscheint diese als bereits intrinsisch modularisiert, sowie in starren Zusammenhängen logisch organisiert, als Ausführbares und Ausführendes. Der zweite Schritt ist die Reformulierung von *queer*, eines politischen und philosophischen Konzepts, als informatisches Konzept: als algorithmisch ausführbar, automatisierbar,

was *queer* operationalisiert (vgl. ebd., 160). Diese Verschiebungen, lässt sich an dieser Stelle bemerken, dürfte Keeling nicht beabsichtigt haben, sind sie doch gegenläufig zu ihrer Verwendung des Begriffs *queer* als dezidiert offenem Projekt, das sie als neue und überraschende Relationen ermöglichend beschreibt, was in Sedgwicks Sinne als reparativ aufgefasst werden kann. Das »ontologische Debakel«, wie es Deuber-Mankowsky (2020; 2017a) darlegt, schließt hingegen Zukünfte, da es die operationalisierten Konzepte durch die Algorithmisierbarkeit und Ausführbarkeit deterministisch werden lässt.

QueerOS: A User's Manual

Ausgehend von diesen Operationalisierungen von *queer* ist es ein vergleichsweise kleiner Schritt zu einem *Queer OS* als Betriebssystem von Computern. Mit ihrem Text *QueerOS: A User's Manual* legen Fiona Barnett, Zach Blas, Micha Cárdenas, Jacob Gaboury, Jessica Marie Johnson und Margaret Rhee (2016) eine Lesart von *Queer OS* vor, die Kara Keelings Überlegungen zum Ausgang nimmt, aber stärker auf ein Verständnis von Queer OS als Betriebssystem von Computern oder mobilen Endgeräten hin denkt. Barnett et al. (ebd., 50) markieren ihren Anfangspunkt als Keelings Definition, »QueerOS would make it impossible to think of phenomena of identitarian difference as separate from information technologies.« Während sie die von Keeling geleistete Auflistung rezenter und im Entstehen begriffener Projekte schätzen, die sich mit der Intersektion und Verstricktheit von Queerness und Technik befassen, diagnostizieren sie dennoch, »QueerOS remains a largely speculative project«, und begreifen diese Unschärfe als »a challenge set forth by Keeling to those who have begun to think these worlds together« (ebd.), derer sie sich in ihrem Aufsatz annehmen.

Was zunächst auffällt ist die Schreibweise *QueerOS*: War bei Keeling noch ein Leerzeichen zwischen *Queer* und dem *Operating System*, so wird hier durch die stilisierte Schreibweise ohne Leerzeichen, die im Artikel durch Zitationen bereits Keeling zugeschrieben wird, schon angedeutet, welche Richtung die Weiterführung von Keelings Konzept einschlägt. *QueerOS* erinnert in dieser Schreibweise an *MacOS*, sowie an die Namen verschiedener Linux-Distributionen.[17] Dennoch positionieren sich die Autor_innen (ebd., 50) explizit als Gegenentwurf zur dominant *weißen* und männlichen, wie auch rassistisch-sexistischen Kultur, die sie mit GNU/Linux assoziieren: »However, our

17 Für eine Auflistung ähnlicher Namen siehe die Webseite *ArchiveOS* (o.J.).

OS doesn't come in the form of GNU/Linux's man pages with detailed descriptions of switches, pipes, and flags.« Die Geste der Absetzung von den GNU/Linux »man pages«, also den *manual pages*, dem Handbuch, entfaltet ihre volle Kraft vor dem Hintergrund des in Linux-Hilfsforen oft verwendeten Akronyms »RTFM«, das ausgeschrieben für »read the fucking manual« steht. RTFM wird oftmals auf von der Community als unnötig oder zu basal empfundene Fragen geantwortet (vgl. The Jargon File o.J.e), und stellt insofern einen Gatekeeping-Mechanismus dar, als außer Acht gelassen wird, dass die GNU/Linux *man pages* oftmals für Anfänger_innen schwer zu verstehen sind. Barnett et al. (2016, 50) möchten ein inklusiveres Projekt entwerfen, das über das Ausborgen der »language of popular software to present an accessible introduction« ein Handbuch für ein neues Betriebssystem bereitstellen möchte, »with each component given a poetic and theoretical description of its features and limitations.« In der Fußnote, mit der dieser Satz versehen ist, weisen die Autor_innen darauf hin, dass manche der von ihnen beschriebenen technischen Features zum Zeitpunkt ihrer Arbeit an dem *User's Manual* (noch) nicht existieren. Nichtsdestotrotz nehmen sie bestehendes Vokabular auf und spinnen dieses mit »performative and disruptive intent« (ebd., 58) weiter. Als Einflüsse für ihr *QueerOS* benennen die Autor_innen neben Kara Keeling auch Vertreter_innen aus Queer Theory, Science-Fiction und Aktivismus, sowie feministische Medienprojekte von Schwarzen Menschen, People of Color und trans Personen (vgl. ebd., 50–51). Im Zuge dessen beziehen sich Barnett, Blas, Cárdenas, Gaboury, Johnson und Rhee (ebd., 51) auf *Queerness* als »socially constructed, promiscuous, political, and discomfiting«, aber auch als »technological, operative, and systemic, derived from individual interests, mutual concern, and discussions that have emerged from collective presentations, virtual discussions, and queer dreams.« An dieser Stelle wiederholt sich die Operationalisierbarkeit von *Queer*, die bereits bei Keeling angelegt war, womit sich die Frage aufwirft, zu welchem Zweck das es operationalisiert wird. Der Einsatz der Autor_innen lässt sich als Versuch, aber auch als Wunsch interpretieren, durch die Operationalisierbarkeit von *Queer* eine Stärkung dieses Konzepts innerhalb einer informatischen Logik zu erzielen: Gehören das philosophische Konzept *Queer* und die informatische Logik beide derselben Ordnung an, so würde sich das Ansteckungspotential von *Queer* auf die Informatik erhöhen (vgl. ebd.). Dennoch ist erkennbar, dass die Autor_innen ein Bewusstsein für die zu vermeidende Verkürzung von *Queer* innerhalb einer solchen Logik haben. So bemerken sie beispielsweise: »Our hope is not to present a unified theory of what a queer operating system should be

[…] this is a speculative proposition for a technical project that does not yet exist and may never come to exist, a project that does not yet function and may never function.« (Ebd.) Als Ziel von *QueerOS* beschreiben Barnett, Blas, Cárdenas, Gaboury, Johnson und Rhee (ebd.), »to address what we perceive as a lack of queer, trans, and racial analysis in the digital humanities, as well as the challenges of imbricating queer/trans/racialized lives and building digital/technical architectures that do not replicate existing systems of oppression.« In dem Wissen, dass *Queer* und *Computation* als Konzepte sich beim Versuch, sie in derselben Ordnung zu situieren, als widerständig erweisen, bezeichnen Barnett et al. (ebd.) ihre Ergebnisse mehr als Denkanstöße, als »theoretical vaporware, speculative potentialware, ephemeral praxis.« *QueerOS* lässt sich damit als ein aktivistisch-ästhetisches Projekt begreifen, das sich gegen die Fortschreibung bestehender sozialer Ungerechtigkeiten in technischen Strukturen richtet, sowie geisteswissenschaftliche Analysen um marginalisierte Positionen erweitern möchte. Dennoch stellt sich die Frage, wie produktiv *QueerOS* für dieses Anliegen sein kann, wenn die Autor_innen einerseits um die Begrenztheit der Operationalisierbarkeit von *Queer* wissen, diese aber trotzdem vornehmen; sowie sich an verschiedenen Stellen gegen die grundsätzliche Logik des informatischen Diskurses richten, aber dennoch dessen Vokabular, und damit dessen Logik übernehmen. *QueerOS* ist damit von einer Unschärfe gekennzeichnet, die Schwierigkeiten mit sich bringt, und im Folgenden genauer betrachtet werden soll.

Im Verlauf ihres Aufsatzes gehen die Autor_innen in sechs Sinnabschnitten auf *Interface*, *User*, *Kernel*, *Applications*, *Memory* und *I/O* ein. Diese werden hier nicht im Detail diskutiert, dennoch sollen exemplarisch die Vermengungen und Unschärfen von *Queer* und Informatik nachgezeichnet werden. Das erste Beispiel befindet sich im Abschnitt zu Interfaces. Barnett et al. (ebd., 52) beziehen sich auf das Interface als zentralen Ort der Zusammenkunft von Menschen und Maschinen, sowie als Ort der Übertragungen zwischen diesen beiden. Trotz dieser besonderen Rolle seien Interfaces »prophylactic, accepting only that which has been made hygienic through a translation from the material world into information.« (Ebd.) Abgesehen von dem anzubringenden Einwand, dass auch Informationen über Materialität verfügen, wird jedoch klar, was Barnett et al. hier adressieren: Informationen, die in einen Computer eingegeben werden können, müssen einer bestimmten Form gehorchen, über eine Medialität verfügen, die bestimmte qualitative Elemente derselben ausschließt. In diesem Sinne fragen die Autor_innen danach, wie ein Interface aussehen könnte, das nicht auf »Shannon's mathematical

theory of communication, but on something disarticulated from Western epistemologies« (ebd.) basiert, in dem die Figur des *störenden Dritten* nicht als ausgeschlossenes Element reproduziert würde, sondern als »that which connects and transforms us, an infectious intimacy in which bodies are open to the transformation that arises from one to another« (ebd.) konfiguriert wäre. Die an dieser Stelle artikulierte Idee, User_innen und Maschine verschmelzen zu lassen, indem die starren und als formatierend erlebten *Grammars of Action* (vgl. Agre 1994) zugunsten eines Interfaces aufgebrochen werden, bei dem »interaction […] might transform both the user and the system« (Barnett et al. 2016, 52), wird kurz darauf zugunsten der Idee eines Interfaces verworfen, das sich unsichtbar macht, aber dennoch nicht naturalisiert (vgl. ebd., 53).[18] *QueerOS* wird im Verlauf des Textes immer wieder in ähnlich paradoxer Weise charakterisiert, entweder durch Stilblüten wie »QueerOS rejects the body and yet requires it« (ebd.), oder durch einander widersprechende Aussagen über technische Möglichkeiten des Systems. So fordern die Autor_innen zwar eine Abkehr von der Shannon'schen Logik der Informationsverarbeitung sowie eine Zurückweisung von Funktionalität und eine Privilegierung von Instabilität (vgl. ebd.), formulieren aber gleichermaßen den Anspruch plattformübergreifender Interoperabilität von Apps (vgl. ebd., 55), die ohne die von ihnen zurückgewiesenen Prinzipien informatischer Logik nicht möglich wären. Es ließen sich noch verschiedene weitere Beispiele anführen, doch diese Untersuchung möchte nicht selbst in ein *paranoid reading* verfallen, in dem akribisch nach den technischen Unmöglichkeiten eines bereits als unscharf und spekulativ markierten ästhetischen Projekts gesucht wird.

Bezugnehmend auf José Esteban Muñoz' (2009) Konzept der *Queer Futurity* formulieren Barnett et al. (2016, 53): »Both user and OS agree there will be no finite in the OS. The OS will be emergent, transformative, and ›not yet here‹.« Zusammenfassend lässt sich an dieser Stelle sagen, dass es sich bei *QueerOS* um ein in erster Linie ästhetisches Projekt handelt, das daher ebenfalls in Sedgwicks Sinne als *reparative reading* verstanden werden kann, insofern es einige Überraschungen bereithält, sowie die Beziehung der Leser_innen zu den beschriebenen Gegenständen neu gestaltet, und in dem sich trotz, oder vielmehr: aufgrund der Unschärfen neue Denkanstöße ergeben. In diesem Sinne bietet *QueerOS* »no permanent solutions, only tactical interventions that

---

18 Angesichts der bereits in Kapitel 2 mit Krämer und Bolter/Grusin besprochenen Logik von Medialität ist zweifelhaft, ob irgendein Medium auf diese Weise existieren könnte, doch um die reine Machbarkeit geht es *QueerOS* nicht.

strive toward a future, becoming a utility that assumes its own obsolescence but which may be refigured, rearranged, and executed once again.« (Ebd., 58) Aus einer technisch informierten Perspektive lässt sich dennoch einwenden, dass die Unschärfe in erster Linie dadurch bedingt ist, dass die *attachments* und Erkenntnisweisen der Informatik zugunsten von *Queer* als philosophisch-aktivistischem Konzept vernachlässigt, oder etwas spitzer formuliert, nicht ernst genommen werden. Barnetts, Blas', Cárdenas', Gabourys, Johnsons und Rhees Versuch, *Queer* nicht vollständig zu operationalisieren und damit einer verflachenden, algorithmischen Logik zu unterwerfen, hat stattdessen zu einer Verflachung des informatischen Diskurses geführt. Für den dritten zu diskutierenden Text der Reihe stellt sich damit die Frage, ob und wie *Queer* und *Computation* in einer Weise miteinander verschränkt werden können, die die jeweiligen Eigenheiten der Diskurse berücksichtigt und anerkennt.

Queer Computation

In seinem 2018 erschienen Artikel *Critical Unmaking: Toward a Queer Computation* fragt Jacob Gaboury nach der Existenz von *Queer Computation* und ihren Modalitäten. Gaboury geht auf verschiedene Möglichkeiten ein, wie *Computation*, also die Art, wie Computer rechnen und funktionieren, aber auch wie sie verwendet und imaginiert werden, queer sein oder gequeert werden könnte. Dazu sei es notwendig, formuliert er, »that we find new ways to make queer theory speak to technology on its own terms.« (Gaboury 2018, 484) Im Zuge dessen nimmt auch Gaboury (ebd.) unter Bezugnahme auf Alexander Galloway explizit eine Operationalisierung von *Queerness* vor:

> »[T]his chapter looks to ›compute queerness‹ by both making it subject to the logic of computation and asking it to act computationally; that is, to become executable. In doing so, it proposes a practice of critical unmaking, foregrounding queer techniques of refusal, misuse, and disruption that must nonetheless work with and through contemporary digital technologies.«

Wie *Queerness* berechenbar und ausführbar gemacht werden könne, führt Gaboury anhand von vier Bereichen aus, die er als Schauplätze von *Queer Computation* identifiziert: den Fail, den Glitch, Normen – in Form von Protokollen – und Code selbst.

Anhand von Jack Halberstams Konzept von *queer failure* beschreibt Gaboury *Queer Computation* in Bezug auf den *Fail* als Möglichkeit, Technik aus einem teleologischen Fortschrittsnarrativ zu lösen. So würde *Queer Computation* sich die Widerständigkeit von *Queerness* zunutze machen, die sich (ironischer Weise) in

dem »refusal to be made useful or productive« (ebd.) ausdrücke. »To compute queerly«, führt Gaboury (ebd., 485) weiter aus,

> »is to acknowledge, embrace, and enact a practice of radical technological failure. It is to engage in critical unmaking: to make central those externalities – exploits, bugs, breakdown, abuse, and misuse – of our digital culture that, while pervasive, we nonetheless disavow. […] In acknowledging, accepting, and even producing failure, queer computation seeks to make clear the values and assumptions that drive our culture of technological development and to offer alternate modes for living with and through technology.«

Aber was kann es eigentlich bedeuten, absichtlich Fehler in digitalen Systemen herzustellen? Um dieser Frage nachzugehen, wendet sich Gaboury dem *Glitch* zu. Ein Glitch ist eine »temporary malfunction« (ebd.), die unerwartet auftritt, und als Störung die Materialität des Mediums offenbart. Nach einigen Überlegungen zur Rolle des Glitchs in Medienkunst bemerkt Gaboury (ebd., 486), die »proliferation of glitch as an aesthetic practice […] diminishes its radical potential«. Betrachtet man Glitches als gewollte ästhetische Phänomene, so riskiere man, ihnen ihr disruptives Moment zu nehmen und normalisiere sie fernab eines radikalen und damit queeren Potentials, das in diesem Beispiel nur ein tatsächlicher Fail haben könne. An dieser Stelle entsteht eine grundlegende Schwierigkeit von *Queer Computation* als Projekt, die Gaboury besonders in Bezug auf *Normen* und *Protokolle* herausarbeitet: Da IT-Systeme standardisiert, und Kommunikation zwischen Computern mit Protokollen, die die Grenzen und Regeln des Sagbaren herstellen (vgl. ebd., 488), bestimmt ist und sein muss, um überhaupt zu funktionieren, kurz: weil digitale Systeme ohne mathematische Exaktheit zum Scheitern verurteilt sind, biete eine Verweigerung dieser Normen wenig Ansatzpunkte für eine queere Kritik von *Computation* abseits von »complete annihilation« (ebd., 486) oder des Luddismus.[19] Beide Optionen betrachtet Gaboury (ebd.) jedoch als nicht zielführend:

> »[…] while it may be compelling to smash our computers in an act of queer rebellion, the radical potential of such a gesture ends there. A broken machine cannot compute, queerly or otherwise. It is a brick, a doorstop; it has no radical potential for computation as it has no computational function.

19 Gerade der Luddismus, denkt man bspw. an das Manifest des sog. »Unabombers« Theodore Kaczynski, zeigt auch eher in die Richtung einer toxischen Männlichkeit als einer queeren Kritik. Vgl. dazu Kaczynski (2010).

> Likewise, it may be compelling to simply opt out of digital technologies altogether, supposing that digital media are irreconcilable with a radical queer politics. While Luddism is certainly a form of critique, it is deeply limited in its efficacy here.«

Dies führt zu *Code* als letztem Bereich von Gabourys Überlegungen zu *Queer Computation*. Anhand einer Diskussion verschiedener Medienkunstprojekte, in deren Zentrum Programmiersprachen stehen, die nicht den für die Informatik gängigen Regeln der Funktionalität folgen, schlägt Gaboury (ebd., 488) vor: »[O]ur queer imperative must be to identify the ideological assumptions that produce protocologial [sic!] norms and then subvert them – to make visible through a queer critical practice the values that structure our technology.« Der Logik von *protocol*, die Alexander Galloway (2004) in seinem gleichnamigen Buch dargelegt hat, folgend, bemerkt Gaboury (2018, 488) weiter: »If it is not possible to work outside the conditions for engagement produced by a given technology, then we must work with technical practices to critique and disrupt the values and assumptions that structure that technology.« Experimentelle Programmiersprachen eignen sich Gaboury (ebd.) zufolge besonders für ein solches Unterfangen, da sie »at the limits of computational logic« operieren, diese aber grundsätzlich erhalten. Eines der von Gaboury (ebd., 489) angeführten Beispiele ist *transCoder*, eine von Zach Blas konstruierte Programmiersprache, die auf »queer linguistic traditions of coded and obfuscated language« basiert, sowie auf Strukturen der Programmiersprache C, und in der Lage sei, ein »double coding« zu erzeugen. »To compute queerness«, schließt Gaboury (ebd., 490) seine Ausführungen,

> »we must begin by acknowledging what queerness offers to a critique of computation. In doing so, we are left with few clear answers and are instead asked to imagine new ways to work against the normalizing influence of our technical culture while maintaining the general functionality of the systems we inhabit.«

Queerness bestimmt Gaboury (ebd.) ebenfalls in Anlehnung an Muñoz »as a means of imagining a future that is not yet here«, weist aber zugleich darauf hin, dass ebendiese Zukünfte durch die »cultural logic of contemporary technology« kolonisiert worden seien, und daher nicht mehr als »primary vector for queer computational critique« funktionieren könnten. Gaboury (ebd.) folgert, »rather than mobilize queerness as a useful technological apparatus, we might deploy it as part of a critical practice of unmaking.« Während der

Ablehnung von »queerness as a useful technological apparatus«, also der Operationalisierung von Queerness, durchaus zuzustimmen ist, soll an dieser Stelle dennoch kritisch angemerkt werden, dass auch die Vorstellung, die Zukunft sei bereits kolonisiert worden, als ein Effekt der Verflachung durch Operationalisierung betrachtet werden kann, die also immer noch am Werk ist: Nur, wenn Queerness als derselben Ordnung wie die Informatik angehörend vorgestellt wird, erscheint ihr Potential als durch diese aufgehoben, erscheinen die Zukünfte als bereits determiniert.

Beide Ansätze Gabourys, sowohl die Operationalisierung von Queerness, die er als nicht zielführend betrachtet, als auch die von ihm vorgeschlagene Auflösung dieses Vorschlags durch die Positionierung von Queerness als »critical practice of unmaking«, sind in Sedgwicks Sinne nicht als reparativ einzustufen. Gegen seine Einordnung von Queerness als »critical practice of unmaking«, also als normative Ordnungen destabilisierendes und denaturalisierendes Element, lässt sich ebenfalls mit Michaelsens (2018, 105) Sedgwick-Lektüre einwenden, dass eine solche Konzeptionalisierung von Queerness auch in anderen Kontexten mit Sedgwick nicht als reparativ verstanden werden kann:

> »Für Sedgwick handelt es sich um eine Fehldeutung, queere Kultur lediglich als Parodie, De-Naturalisierung und Verspottung von dominanter Kultur zu betrachten. […] Einer Perspektive, die sich auf das Entlarven und das ›Immerschon‹ von Macht und Gewaltförmigkeit fokussiert, entgehen diese reparativen Elemente queerer Existenz.«

Reparativ wäre stattdessen, wie Michaelsen (ebd., 112) ausführt, eine »Betonung des Medienspezifischen und Materiellen«, die zum sinnlichen und ästhetischen Überschuss zurückführe. »Möglicherweise«, bemerkt Michaelsen (ebd., 114) an anderer Stelle, »beziehen sich Scheitern und Überschuss auf dasselbe, nur einmal in paranoidem und einmal in reparativem Vokabular.« Zum Überschuss schreibt sie weiter:

> »Medientheoretisch ist mit Überschuss der Anteil des Medialen an dem gemeint, was es vermittelt bzw. was nicht ganz in dem Vermittelten aufgeht. Als solches ist es für die Konstitution des Vermittelten entscheidend und produziert einen Sinn-Überschuss. Dieser manifestiert sich insbesondere in Momenten der Störung, in denen sich die Materialität des Mediums zeigt, im Rauschen, in Pixeln etc.« (Ebd., 112)

Dieser Hinweis ist vor allem vor dem Hintergrund von Gabourys Perspektive auf den Glitch von Interesse: Wenn Gaboury den Glitch als Moment von Queer-

ness verwirft, da dieser Queerness scheinbar normalisiere und seines disruptiven Potentials beraube, ist dies ebenso eine nicht-reparative Perspektive auf Queerness wie ihre Operationalisierung.

Mit Deuber-Mankowsky (2017a, 163–164, 167) wurde bereits darauf hingewiesen, dass die Operationalisierung analytischer Begrifflichkeiten zu einer Unschärfe in der Theoriebildung führt, die gerade in Bezug auf digitale Medien mit einem instrumentellen Technikverständnis einhergeht, in dem Technik als Werkzeug und damit als beherrschbar erscheint. Bei Gaboury, so ließe sich argumentieren, liegt die Gefahr eines durch die Operationalisierung erzeugten instrumentellen Verständnisses von Queerness vor, die damit vorrangig als Mittel, als bloßes Werkzeug zur denaturalisierenden Machtanalyse konzeptualisiert, und infolgedessen als philosophisches Projekt und als Lebensrealität stillgestellt wird. Eine reparative Perspektive würde jedoch außerhalb einer Operationalisierung von Queerness und dem aus der Operationalisierung gesuchten Ausweg, Queerness als die informatische Logik denaturalisierend zu begreifen, stattfinden. Denn, wie Michaelsen (2018, 113) in Bezug auf eventuelle reparative Anschlüsse in medienwissenschaftlicher Geschlechterforschung konstatiert, werden diese gerade durch das »besondere Interesse am medialen und materiellen Überschuss« möglich:

> »Gerade die dabei in den Blick rückenden Ästhetiken und Affekte, die auf Bedeutung jenseits hegemonialer semantischer Inhalte hinweisen, sind als lebenserhaltende Ressourcen u.a. für unterdrückte und marginalisierte Gruppen zu verstehen. Die Frage wäre nicht nur, welchen Anteil das Mediale an Konzepten von Geschlecht hat bzw. wie sich Gender und Medien wechselseitig konstituieren. Das Interesse würde sich stattdessen auf den medialen Anteil richten, der über die Wiederholung und Verfestigung normativer Geschlechter hinausgeht. Das dadurch produzierte Wissen kann als reparativ verstanden werden, da es einen anderen, weniger ausschließlich auf Machteffekte ausgerichteten Blick ermöglicht bzw. deren allumfassende Wirkmächtigkeit infrage stellt.« (Ebd.)

5.2.2 Queere Sicherheit

Anhand der bisher angestellten Überlegungen zu *Queer OS*, *QueerOS* und *Queer Computation* lässt sich folgern, dass die diskutierten Versuche, *Queer* und *Computation* zusammenzudenken, zwar an manchen Stellen über reparative Momente verfügen, aber dennoch in weiten Teilen durch die Unschärfen der Theo-

riebildung tendenziell eher in die gegenläufige Richtung zeigen. In allen diskutierten Texten ist eine Operationalisierung von Queerness zu beobachten, die von dem Wunsch getragen ist, Queerness und Informatik in einen Dialog zu bringen, dabei allerdings einen tatsächlichen Austausch verhindert, da beide als bereits denselben Rationalitäten angehörend, das heißt: denselben »Regeln und Prozessen« (Deuber-Mankowsky 2020, 135) folgend, gedacht werden. Diese unscharfe Vermengung führt, wie mit Deuber-Mankowsky argumentiert wurde, zu einer Bedeutungsverschiebung, an deren Ende entweder ein verkürztes Verständnis von *Queer/ness* oder von Technik steht. Das Insistieren der letzten beiden diskutierten Aufsätze, Queerness mit Muñoz (2009, 1) als zukünftig, als »not yet here«, als offene, utopische Zukünfte beinhaltend denken zu wollen, erweist sich damit als durch die Theoriebildung verstellt. Dabei wäre der Einsatz von Queerness als offen und Zukünfte ermöglichend, wie Muñoz (ebd., 12) selbst bemerkt, »aligned with what Sedgwick would call reparative hermeneutics.« Für den Erhalt von Queerness als offen gilt es also, eine ungenaue Übertragung von Konzepten zwischen Queer Theory und Informatik zu vermeiden – beide gehören differenten Bereiche der Wissensproduktion und damit getrennten Wissensordnungen an, die in einer »diskontinuierliche[n] Struktur« (Deuber-Mankowsky 2020, 136) verbunden sind. Unter Bezugnahme auf Sedgwick lässt sich an dieser Stelle noch hinzufügen, dass eine Vermengung beider Bereiche für das Einnehmen einer reparativen Perspektive nicht einmal notwendig ist. Mit Sedgwicks (2003, 124) Bemerkung, ein Verständnis für einen Sachverhalt »does not intrinsically or necessarily enjoin that person to any specific train of epistemological or narrative consequences«, soll an dieser Stelle zur eingangs gestellten Frage nach der Möglichkeit eines queeren, reparativen Sicherheitsbegriffs für die IT-Sicherheit zurückgekehrt werden.

Ein Verständnis für die Rationalität der technisch-informatischen Zusammenhänge, deren Wissensproduktion bereits mit Sedgwick als einer paranoiden Struktur folgend charakterisiert wurde, bedeutet auch, nicht per se an die »epistemological or narrative consequences« des IT-Sicherheitsdiskurses gebunden zu sein. Dies erlaubt es, die eingangs gestellte Frage noch einmal im Wortlaut aufzugreifen: (Wie) kann ein queerer Sicherheitsbegriff für die IT-Sicherheit in Stellung gebracht werden? Auf diese Frage soll basierend auf den bisherigen Überlegungen in drei Punkten geantwortet werden.

Erstens: Es kann nicht darum gehen, IT-Sicherheit mit einem queeren Sicherheitsbegriff neu zu konzeptualisieren, da die Funktionsweise von IT-Sicherheit, wie sie in der vorliegenden Untersuchung beschrieben wurde, ein

Produkt der Kryptologie und der Informatik ist, und bei allen problematischen Eigenschaften des paranoid strukturierten Diskurses nicht einfach anders gedacht werden kann. Ein solcher Versuch würde unweigerlich, wie in diesem Kapitel anhand von *QueerOS* und *Queer Computation* gezeigt wurde, eine Operationalisierung des queeren Sicherheitsbegriffs zur Folge haben, die zu vermeiden ist. Kurz: *Es kann nicht um eine technische Implementierung eines queeren Sicherheitsbegriffs gehen*.

Zweitens: *Statt über queere IT-Sicherheit nachzudenken, lohnt es sich eher, über queere Sicherheitspraktiken im Zusammenhang mit digitalen Kulturen nachzudenken*. Auf diese Weise wird der negative Sicherheitsbegriff der informatischen Logik der IT-Sicherheit als *Sicherheit vor* aufrechterhalten, und gleichzeitig anerkannt, dass das »anti-soziale und damit risikoreiche Moment« (Loick 2021, 278) digitaler Kulturen im Sinne einer »Dekonstruktion der strikten Opposition von Sicherheit und Unsicherheit, durch einen Platz für Negativität im Positiven« (ebd.), notwendiger Bestandteil des Lebens in und mit digitalen Kulturen ist, sowie die Voraussetzung dafür, Sicherheit überhaupt herstellen zu können. Das Wissen um die paranoide Strukturierung der IT-Sicherheit bedeutet damit weiterführend mit Sedgwick nicht, dass diese sich in den Nutzungspraktiken digitaler Medien fortsetzen muss, auch, wenn paranoide Strukturen, wie sie anmerkt, durchaus ansteckend sein können.

Dies führt zu Drittens: Der Verortung von queerer Sicherheit in Bezug auf IT-Sicherheit in den Denkweisen von Sicherheit in digitalen Kulturen, und damit den Umgangsweisen mit vernetzten Computern, und Technik im Allgemeinen. In Anlehnung an Loicks (ebd., 279) Ausführungen über von der queeren Community angesichts der AIDS-Krise entwickelten »konkrete[n] solidarische[n] Fürsorge- und Pflegetätigkeiten«, möchte ich an dieser Stelle vorschlagen, *solidarische Fürsorge- und Pflegepraktiken für das Leben in digitalen Kulturen und mit vernetzten Computern zu entwickeln*. Dies würde bedeuten, kein instrumentelles Technikverständnis zu veranschlagen, in dem (digitale) Medien als bloße Werkzeuge in Erscheinung treten, sowie anzuerkennen, dass das Leben in und mit Technik ebenfalls (System-)Pflegepraktiken beinhalten muss. Diese Fürsorgepraktiken entsprächen damit nicht den Praktiken von *Safe Hex*, die letztlich vereinzelnd wirken, da sie lediglich auf die Eigenverantwortung der User_innen rekurrieren. Stattdessen geht es um reparative, solidarische Praktiken, die unter anderem gekennzeichnet sind von gemeinsamen, unterstützenden (Ein-)Übungen von Nutzungsweisen, von Offenheit für Überraschungen, von anerkannten geteilten Verantwortlichkeiten, sowie davon, Neues auszuprobieren, mit Technik zu spielen, Infrastrukturen

gemeinschaftlich zu konzipieren, zu bauen und zu pflegen, und schließlich über die Anerkennung der Differenzen von Menschen und Maschinen der Unsicherheit, der Negativität, einen Platz in der Herstellung von Sicherheit einzuräumen.

6. Schluss

> Eine reparative Perspektive geht von dem offensichtlichen Umstand aus, dass unsere Welt beschädigt und gefährlich ist, aber anstelle einer *bloßen Wiederholung* von ›bad news‹ zielt sie darauf, eine unterstützende Beziehung zu den Objekten in unserer Umgebung zu ermöglichen, was die ungewöhnliche Forderung nach Liebe als Grundlage der eigenen wissenschaftlichen Arbeit begründet. *(Michaelsen 2018, 99, Herv. i.O.)*

Angefangen bei der Kryptologie über die Geschichte der IT-Sicherheit, über das Zusammentreffen der beiden Bereiche in Kryptovirologie (Ransomware) und Kleptographie (Backdoors) bis hin zu den Versuchen, Queerness und Technik zusammenzudenken, hat die vorliegende Untersuchung entlang der Achsen negativer und queerer Sicherheitsbegriffe sowie paranoider und reparativer Praktiken der Wissensproduktion die Frage diskutiert, wie Sicherheit in digitalen Kulturen organisiert ist und sein könnte. Dabei wurden Brücken zwischen differenten Fachkulturen, und damit unterschiedlichen Formen der Wissensproduktion und -organisation, zwischen unterschiedlichen Rationalitäten und Attachments geschlagen: Zwischen mathematisch-informatischem Wissen und einer stark durch die Queer Theory beeinflussten Medienwissenschaft, was nicht zuletzt durch die reparative Praktik, Liebe als Grundlage der eigenen wissenschaftlichen Arbeit zu begreifen, möglich wurde.

Der Sicherheitsbegriff von Kryptologie und IT-Sicherheit wurde im Verlauf der Untersuchung als negativer Sicherheitsbegriff bestimmt. Anhand der kryptographischen Modellbildung im Fachbereich *Beweisbare Sicherheit* und vor dem Hintergrund der Medialität von Kryptographie wurde der Vorgang der Reduktion besprochen, sowie die Figur des *störenden Dritten*, die aus dem unsicheren Kanal eines gegebenen Systems ausgeschlossen werden muss, als leitende Idee der Kryptologie beschrieben. Für die Phase der Herausbildung der IT-Sicherheit in den 1980er Jahren spielt das *störende Dritte* und dessen Ausschluss aus den mittlerweile vervielfachten unsicheren Kanälen ebenfalls eine maßgebliche Rolle, und wurde anhand einer starken Bezugnahme auf den heteronormativen Mainstream-Diskurs über HIV und AIDS, und damit auf das Immunsystem als Figuration der Differenzgenerierung und auf die Herstellung von Sicherheit für vernetzte Computer übertragen. IT-Sicherheit, so konnte anhand der Konzeptionalisierung von Schadsoftware sowie des Umgangs mit derselben gezeigt werden, imaginiert Computer als Körper, die angesichts dessen allerhand diskursiven und materiellen Ansteckungspotentialen ausgesetzt sind. Den homophoben Elementen des zur Zeit der AIDS-Krise dominanten Diskurses folgend, nimmt die IT-Sicherheit die User_innen in die Pflicht, eigenverantwortlich für die Sicherheit ihrer Maschinen zu sorgen, und, durch die bereits genannten Ansteckungspotentiale, auch für ihre eigene.

Mathematisch-technische Konzeptualisierungen von Sicherheit in digitalen Kulturen folgen also einem negativen Sicherheitsbegriff, und sind darüber hinaus durch paranoide Praktiken der Wissensproduktion gekennzeichnet. Paranoia erfüllt in diesem Zusammenhang sowohl für die Kryptologie als auch die IT-Sicherheit eine doppelte Rolle: Zum einen kann negative Sicherheit nur durch das Antizipieren einer Bedrohung gedacht werden. Zum anderen dient die durch paranoide Praktiken versuchte Vermeidung negativer Affekte der Selbstversicherung des Diskurses, in den die Unsicherheit, und damit die negativen Affekte, trotz aller Bemühungen immer wieder einbrechen. Die paranoiden Praktiken der Wissensproduktion sind damit konstitutiv für die den Kryptologie- und IT-Sicherheitsdiskurs kennzeichnende Überbietungslogik negativer Sicherheit.

Nachdem durch die Diskussion von Backdoors dieser Diskurs für Fragen nach einem möglichen anderen Sicherheitsbegriff geöffnet wurde, konnte anhand von *QueerOS* und *Queer Computation* zunächst herausgearbeitet werden, dass der Versuch, reparative Praktiken in der Form einer Einführung von Queerness in die Logik der Informatik zu denken, kein gangbarer Weg für

eine Neubestimmung von Sicherheit in digitalen Kulturen sein kann. Infolgedessen hat die vorliegende Untersuchung den Fokus von dem Versuch, einen queeren Sicherheitsbegriff innerhalb der IT-Sicherheit zu etablieren, hin zu den Modalitäten queerer Sicherheit in und mit digitalen Kulturen verschoben, sowie tentative Ideen für die Möglichkeit eines solchen skizziert. Der Einsatz eines queeren Sicherheitsbegriffs würde darin liegen, im Gegensatz zu einem paranoid strukturierten, negativen Sicherheitsbegriff, genau nicht einer fortifizierenden Überbietungslogik zu folgen, in der die für die Herstellung von Sicherheit permanent erforderlichen Grenzaushandlungen zwischen vernetzten Computern untereinander, aber auch zwischen Computern und User_innen letztlich in der Eigenverantwortung derselben liegen. Ein queerer Sicherheitsbegriff legt stattdessen Wert auf eine solidarische Herstellung von Sicherheit, an der Menschen und Computer gemeinsam beteiligt sind, und die nur durch die Anerkennung von immer schon gegebener Unsicherheit als Bedingung für die Herstellung von Sicherheit möglich wird. Weiterführend gilt es, Praktiken queerer Sicherheit in und mit digitalen Medien und Systemen zu entwerfen, die nicht auf der Ebene des Technischen angesiedelt sind, aber dennoch über ein genaues Wissen der technischen Funktionsweisen verfügen. Infolgedessen bleibt an dieser Stelle nur noch, zu weiteren Überlegungen und Unternehmungen aufzurufen, die sich in reparativer Weise mit Fragen nach Sicherheit in und mit digitalen Kulturen auseinandersetzen. Damit schließt diese Untersuchung so, wie sie auch mit Marais und Haraway (1997, 123) begonnen hat: »For thus, all things must begin with an act of love.«

Literatur und weitere Quellen

Abbate, Janet. 1999. *Inventing the Internet*. London: The MIT Press.

Adams, Anne, und Martina Angela Sasse. 1999. »Users Are Not the Enemy«. *Communications of the ACM* 42 (12): 40–46. https://doi.org/10.1145/322796.322806.

Agre, Philip E. 1994. »Surveillance and Capture: Two Models of Privacy«. *The Information Society* 10 (2): 101–27. https://doi.org/10.1080/01972243.1994.9960162.

Andreas, Michael. 2014. »›Offen‹ und ›Frei‹. Über zwei Programme sozialer Medien«. In *Soziale Medien – Neue Massen*, herausgegeben von Inge Baxmann, Timon Beyes, und Claus Pias, 151–65. Zürich/Berlin: diaphanes.

ArchiveOS. o.J. »Linux A-D – ArchiveOS«. https://archiveos.org/linux/ (10.05.2021).

Ars Staff. 2013. »Report: NSA paid RSA to make flawed crypto algorithm the default«. *Ars Technica*, 21. Dezember 2013. https://arstechnica.com/information-technology/2013/12/report-nsa-paid-rsa-to-make-flawed-crypto-algorithm-the-default/ (10.05.2021).

Auerbach, Benedikt, Mihir Bellare, und Eike Kiltz. 2018. »Public-Key Encryption Resistant to Parameter Subversion and Its Realization from Efficiently-Embeddable Groups«. In *Public-Key Cryptography – PKC 2018*, herausgegeben von Michel Abdalla und Ricardo Dahab, 348–77. Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-76578-5_12.

Ball, James, Julian Borger, und Glenn Greenwald. 2013. »Revealed: how US and UK spy agencies defeat internet privacy and security«. *The Guardian*, 6. September 2013. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (10.05.2021).

Barabási, Albert-László. 2002. *Linked: The New Science Of Networks Science Of Networks*. Cambridge, MA: Perseus Publishing.

Barnett, Fiona, Zach Blas, Micha Cárdenas, Jacob Gaboury, Jessica Marie Johnson, und Margaret Rhee. 2016. »QueerOS: A User's Manual«. In *Debates in the Digital Humanities*, herausgegeben von Matthew K. Gold und Lauren F. Klein, 50–59. Minneapolis: University of Minnesota Press.

Bauer, Friedrich. 1997. *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. 2. Aufl. Berlin/Heidelberg: Springer.

Bellare, Mihir, Kenneth G. Paterson, und Phillip Rogaway. 2014. »Security of Symmetric Encryption against Mass Surveillance«. In *Advances in Cryptology – CRYPTO 2014*, herausgegeben von Juan A. Garay und Rosario Gennaro, 1–19. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-44371-2_1.

Bergermann, Ulrike. 2016. *Leere Fächer. Gründungsdiskurse in Kybernetik und Medienwissenschaft*. Münster: Lit Verlag. https://doi.org/10.25969/mediarep/14841.

Bergermann, Ulrike. 2018. »biodrag. Turing-Test, KI-Kino und Testosteron«. In *Machine Learning. Medien, Infrastrukturen und Technologien der Künstlichen Intelligenz*, herausgegeben von Christoph Engemann und Andreas Sudmann, 339–64. Bielefeld: transcript.

Berlant, Lauren. 2011. *Cruel Optimism*. Durham: Duke University Press.

Bernstein, Daniel, Tanja Lange, und Ruben Niederhagen. 2015. »Dual EC: A Standardized Back Door«. https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf (10.05.2021).

Bersani, Leo. 1987. »Is the Rectum a Grave?« *October* 43: 197–222. https://doi.org/10.2307/3397574.

Beyes, Timon, und Claus Pias. 2014. »Transparenz und Geheimnis«. *Zeitschrift für Kulturwissenschaften*, Nr. 2: 111–17.

Bickenbach, Matthias, und Harun Maye. 2009. *Metapher Internet. Literarische Bildung und Surfen*. Berlin: Kadmos.

Black, Max. 1962. *Models and Metaphors: Studies in Language and Philosophy*. Ithaca: Cornell University Press.

Bloomfield, Robin, Kateryna Netkachova, und Robert Stroud. 2013. »Security-Informed Safety: If It's Not Secure, It's Not Safe«. In *Software Engineering for Resilient Systems*, herausgegeben von Anatoliy Gorbenko, Alexander Romanovsky, und Vyacheslav Kharchenko, 17–32. Berlin, Heidelberg: Springer.

Blum, Manuel. 1983. »Coin flipping by telephone. A protocol for solving impossible problems«. *ACM SIGACT News* 15 (1): 23–27. https://doi.org/10.1145/1008908.1008911.

Blumenberg, Hans. 1997. *Paradigmen zu einer Metaphorologie*. 7. Edition. Frankfurt a.M.: Suhrkamp Verlag.

Bolter, Jay David, und Richard Grusin. 2000. *Remediation. Understanding New Media*. Cambridge, MA: MIT Press.

Boomen, Marianne van den. 2014. *Transcoding the Digital: How Metaphors Matter in New Media*. Amsterdam: Institute of Network Cultures.

Brandom, Russell. 2017. »Almost All WannaCry Victims Were Running Windows 7«. *The Verge*. 19. Mai 2017. https://www.theverge.com/2017/5/19/15665488/wannacry-windows-7-version-xp-patched-victim-statistics (10.05.2021).

Brandt, Christina. 2004. *Metapher und Experiment. Von der Virusforschung zum genetischen Code*. Göttingen: Wallstein Verlag.

Brazzell, Melanie. 2019. *Was macht uns wirklich sicher? Ein Toolkit zu intersektionaler, transformativer Gerechtigkeit jenseits von Gefängnis und Polizei*. 2. Auflage. Münster: edition assemblage.

Briegleb, Volker. 2017. »Ransomware WannaCry befällt Rechner der Deutschen Bahn«. *Heise Online*, 13. Mai 2017. https://www.heise.de/ho/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html (10.05.2021).

BSI. 2016. »Ein Praxis-Leitfaden für IS-Penetrationstests«. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf;jsessionid=84D00F5F0B70F385B7C9FA57BE728E21.2_cid503?__blob=publicationFile&v=10 (10.05.2021).

BSI. o.J.a »Backdoor«. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html (10.05.2021).

BSI. o.J.b. »IT-Grundschutz. SYS. 4.4 Allgemeines IoT-Gerät«. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_4_Allgemeines_IoT-Ger%C3%A4t.html (10.05.2021).

Butler, Judith. 2002. »Performative Akte und Geschlechterkonstitution. Phänomenologie und feministische Theorie«. In *Performanz. Zwischen Sprachphilosophie und Kulturwissenschaften*, herausgegeben von Uwe Wirth, 301–20. Frankfurt a.M.: Suhrkamp.

Caloyannides, Michael A. 2004. *Privacy Protection and Computer Forensics*. 2. Aufl. Boston/London: Artech House.

Cameron, Dell. 2017. »Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It«. *Gizmodo Australia*, 13. Mai 2017. https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/ (10.05.2021).

Chebyshev, Victor, Evgeny Lopatin, Fedor Sinitsyn, Alexander Liskin, Denis Parinov, und Oleg Kupreev. 2018. »IT threat evolution Q3 2018. Statistics«. 12. November 2018. https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/ (10.05.2021).

Chua, Joyce. 2017. »Tackling Ransomware Attacks«. https://www.rsaconference.com/writable/presentations/file_upload/tta-f04_tackling-ransomware-attacks.pdf (10.05.2021).

Chun, Wendy Hui Kyong. 2006. *Control and freedom: power and paranoia in the age of fiber optics*. Cambridge, Mass.: MIT Press.

Chun, Wendy Hui Kyong. 2012. »Race and/as Technology or How to Do Things to Race«. In *Race After the Internet*, herausgegeben von Lisa Nakamura und Peter Chow-White, 38–60. New York/London: Routledge.

Cifor, Marika, und Cait McKinney. 2020. »Reclaiming HIV/AIDS in Digital Media Studies«. *First Monday*, September. https://doi.org/10.5210/fm.v25i10.10517.

CISO, Joe. 2018. »Emotet — The Polymorph Strikes Back«. *Medium*. 12. April 2018. https://medium.com/@JoeCISO/emotet-the-polymorph-strikes-back-1e25d80abfd9 (10.05.2021).

Clark, Zammis. 2017. »The Worm That Spreads WanaCrypt0r«. *Malwarebytes Labs*. 12. Mai 2017. https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/ (10.05.2021).

Cloudflare. o.J.a. »How Do Lava Lamps Help with Internet Encryption?« *Cloudflare*. https://www.cloudflare.com/learning/ssl/lava-lamp-encryption/ (10.05.2021).

Cloudflare. o.J.b. »What is the Mirai Botnet?« *Cloudflare*. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ (10.05.2021).

Cohen, Fred. 1987. »Computer Viruses: Theory and Experiments«. *Computers & Security* 6 (1): 22–35. https://doi.org/10.1016/0167-4048(87)90122-2.

Cormen, Thomas. 2013. *Algorithms Unlocked*. Cambridge (Massachusetts); London (England): The MIT Press.

Crimp, Douglas. 1987a. »How to Have Promiscuity in an Epidemic«. *October* 43: 237–71. https://doi.org/10.2307/3397576.

Crimp, Douglas. 1987b. »Introduction«. *October* 43: 3–16. https://doi.org/10.2307/3397562.

Cult of the Dead Cow. 1998a. »RUNNING A MICROSOFT OPERATING SYSTEM ON A NETWORK? OUR CONDOLENCES.«. https://web.archive.org/web/19981205234956/www.cultdeadcow.com:80/news/back_orifice.txt (10.05.2021).

Cult of the Dead Cow. 1998b. »Worst Case Scenario – BUTTplug«. https://web.archive.org/web/19981206051049/www.cultdeadcow.com/tools/bo_plugins.html (10.05.2021).

danooct1. 2012a. *Virus.DOS.Jerusalem (Friday the 13th Special)*. https://www.youtube.com/watch?v=u3k-8kJ54sg (10.05.2021).

danooct1. 2012b. *Virus.DOS.Cascade*. https://www.youtube.com/watch?v=z7g-v3d7-Gk (10.05.2021).

Degabriele, Jean Paul, Pooya Farshim, und Bertram Poettering. 2015. »A More Cautious Approach to Security Against Mass Surveillance«. In *Fast Software Encryption*, herausgegeben von Gregor Leander, 579–98. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-48116-5_28.

Delpy, Benjamin. 2017. »wanakiwi: Automated wanadecrypt with key recovery if lucky«. Github. https://github.com/gentilkiwi/wanakiwi (10.05.2021).

Derrida, Jacques. 1983. *Grammatologie*. Übersetzt von Hans-Jörg Rheinberger und Hanns Zischler. 14. Edition. Frankfurt a.M.: Suhrkamp.

Deuber-Mankowsky, Astrid. 2017a. »Das ontologische Debakel oder was heißt: Es gibt Medien?« *Zeitschrift für Medien- und Kulturforschung* 8 (2): 157–67. https://doi.org/10.28937/1000107979.

Deuber-Mankowsky, Astrid. 2017b. *Queeres Post-Cinema. Yael Bartana, Su Friedrich, Todd Haynes, Sharon Hayes*. Berlin: August Verlag.

Deuber-Mankowsky, Astrid. 2020. »›Für eine Maschine gibt es kein echtes Virtuelles‹. Zur Kritik des Smartness Mandate mit Felwine Sarrs Afrotopia und Gilbert Simondons Philosophie der Technik«. *Internationales Jahrbuch für Medienphilosophie* 6 (1): 131–46.

Diffie, Whitfield, und Martin Hellman. 1976. »New directions in cryptography«. *IEEE Transactions on Information Theory* 22 (6): 644–54. https://doi.org/10.1109/TIT.1976.1055638.

Diffie, Whitfield, und Susan Landau. 2007. »The Export of Cryptography in the 20th and the 21st Centuries«. In *The History of Information Security: A Comprehensive Handbook*, herausgegeben von Karl de Leeuw und Jan Bergstra, 725–36. Amsterdam: Elsevier.

Doll, Martin. 2012. *Fälschung und Fake. Zur diskurskritischen Dimension des Täuschens*. Berlin: Kadmos.

Dozier, Rob. 2019. »A Computer Afflicted With 6 Infamous Viruses Has Passed $1 Million at Auction«. *Motherboard*, 21. Mai 2019. https://www.vice.com/en/article/vb93jx/a-computer-afflicted-with-6-infamous-viruses-has-passed-dollar1-million-at-auction (10.05.2021).

Draude, Claude. 2017. *Computing Bodies: Gender Codes and Anthropomorphic Design at the Human-Computer Interface*. Berlin: Springer.

Dudenredaktion. 2018. »Hintertür, die«. Duden online. https://www.duden.de/node/66793/revision/66829 (10.05.2021).

Dudenredaktion. 2020. *Duden. Das Fremdwörterbuch*. 12., Vollständig überarbeitete und Erweiterte Ausgabe. Berlin: Bibliographisches Institut GmbH. http://ebookcentral.proquest.com/lib/uni-bochum/detail.action?docID=6363333 (10.05.2021).

DuPont, Quinn, und Alana Cattapan. 2017. »Alice and Bob: A History Of The World's Most Famous Couple«. http://cryptocouple.com/Alice%20and%20Bob%20-%20DuPont%20and%20Cattapan%202017.pdf (10.05.2021).

DuPont, Quinn. 2017. »An Archeology of Cryptography: Rewriting Plaintext, Encryption, and Ciphertext«. Dissertation an der University of Toronto. https://tspace.library.utoronto.ca/handle/1807/78958 (10.05.2021).

DuPont, Quinn. 2020. »Cryptographic Media«. In *Second International Handbook of Internet Research*, herausgegeben von Jeremy Hunsinger, Matthew M. Allen, und Lisbeth Klastrup, 691–705. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-024-1555-1_34.

Ebert, Roger. 1994. »Body Snatchers Movie Review & Film Summary (1994)«. https://www.rogerebert.com/reviews/body-snatchers-1994 (10.05.2021).

Elmer-Dewitt, Philip. 1988. »Invasion of the Data Snatchers«. *Times*, 26. September 1988. http://content.time.com/time/subscriber/printout/0,8816,968508,00.html (10.05.2021).

Ernst, Wolfgang. 2000. »Umbrella Word oder wohldefinierte Disziplin? Perspektiven der ›Medienwissenschaft‹«. *MEDIENwissenschaft: Rezensionen | Reviews* Jg. 17 (1): 14–24. https://doi.org/10.17192/ep2000.1.2797.

Ernst, Wolfgang. 2018. »Das Wissen von Medien und seine techno-logische Erdung«. In *Medientechnisches Wissen, Band 1: Logik, Informationstheorie*, herausgegeben von Stefan Höltgen, 5–12. Berlin, Boston: De Gruyter Oldenbourg. https://doi.org/10.1515/9783110477504.

Ferbrache, David. 1992. *A Pathology of Computer Viruses*. London: Springer.

Fischer, Lars. 2017. »Bio-Hacking: Computervirus aus DNA greift Software an«. *Spektrum.de*, 11. August 2017. https://www.spektrum.de/news/computervirus-aus-dna-greift-software-an/1493621 (10.05.2021).

Flichy, Patrice. 1994. *Tele. Geschichte der modernen Kommunikation*. Frankfurt/New York: Campus Verlag.

Folkers, Andreas. 2020. »Eine Genealogie sorgender Sicherheit. Sorgeregime von der Antike bis zum Anthropozän«. *BEHEMOTH. A Journal on Civilisation* 13 (2): 16–39. https://doi.org/10.6094/behemoth.2020.13.2.1044.

Forrest, Stephanie, Steven A. Hofmeyr, und Anil Somayaji. 1997. »Computer Immunology«. *Communications Of The ACM* 40 (10): 88–96.

Foucault, Michel. 1996. *Diskurs und Wahrheit: die Problematisierung der Parrhesia. Sechs Vorlesungen, gehalten im Herbst 1983 an der Universität von Berkeley/Kalifornien*. Berlin: Merve.

Foucault, Michel. 2006. *Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I*. 1. Aufl. Frankfurt a.M.: Suhrkamp.

Fox-Brewster, Thomas. 2017. »Medical Devices Hit By Ransomware For The First Time In US Hospitals«. *Forbes*, 17. Mai 2017. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/ (10.05.2021).

Freud, Sigmund. 1955. *Psychoanalytische Bemerkungen über einen Autobiographisch Beschriebenen Fall von Paranoia (Dementia Paranoides)*. Bd. VIII. Gesammelte Werke. London: Imago Publishing.

Gaboury, Jacob. 2013a. »A Queer History of Computing«. *Rhizome*. https://rhizome.org/editorial/2013/feb/19/queer-computing-1/ (10.05.2021).

Gaboury, Jacob. 2013b. »A Queer History of Computing, Part Five: Messages from the Unseen World«. *Rhizome*. https://rhizome.org/editorial/2013/jun/18/queer-history-computing-part-five/ (10.05.2021).

Gaboury, Jacob. 2013c. »A Queer History of Computing: Part Four«. *Rhizome*. https://rhizome.org/editorial/2013/may/6/queer-history-computing-part-four/ (10.05.2021).

Gaboury, Jacob. 2013d. »A Queer History of Computing: Part Three«. *Rhizome*. https://rhizome.org/editorial/2013/apr/9/queer-history-computing-part-three/ (10.05.2021).

Gaboury, Jacob. 2013e. »A Queer History of Computing: Part Two«. *Rhizome*. https://rhizome.org/editorial/2013/mar/19/queer-computing-2/ (10.05.2021).

Gaboury, Jacob. 2018. »Critical Unmaking: Toward a Queer Computation«. In *The Routledge Companion to Media Studies and Digital Humanities*, herausgegeben von Jentery Sayers, 483–91. New York/London: Routledge, Taylor & Francis Group.

Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization*. Illustrated Edition. Cambridge, Mass.: The MIT Press.

Galloway, Alexander R., und Eugene Thacker. 2007. *The Exploit: A Theory of Networks*. Minneapolis: University of Minnesota Press.

Garfinkel, Simson, und Heather Richter Lipford. 2014. *Usable Security: History, Themes, and Challenges*. San Rafael: Morgan & Claypool Publishers.

Gazet, Alexandre. 2010. »Comparative analysis of various ransomware virii«. *Journal in Computer Virology* 6 (1): 77–90. https://doi.org/10.1007/s11416-008-0092-2.

Gießmann, Sebastian. 2016. *Die Verbundenheit der Dinge. Eine Kulturgeschichte der Netze und Netzwerke*. 2. Aufl. Berlin: Kadmos.

Gilman, Sander L. 1987. »AIDS and Syphilis: The Iconography of Disease«. *October* 43: 87–107. https://doi.org/10.2307/3397566.

Goldreich, Oded. 2004. *Foundations of Cryptography. Basic Tools*. Cambridge: Cambridge University Press.

Goldreich, Oded. 2009. *Foundations of Cryptography II: Basic Applications*. Cambridge: Cambridge University Press.

Goldreich, Oded. 2012. »On Post-Modern Cryptography«. *Cryptology ePrint Archive*, 1–12. http://www.wisdom.weizmann.ac.il/~oded/PDF/on-pmc1.pdf (10.05.2021).

Goldwasser, Shafi, und Silvio Micali. 1982. »Probabilistic encryption & how to play mental poker keeping secret all partial information«. In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, 365–77. STOC '82. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/800070.802212.

Goldwasser, Shafi, und Silvio Micali. 1984. »Probabilistic Encryption«. *Journal of Computer and System Sciences* 28 (2): 270–99. https://doi.org/10.1016/0022-0000(84)90070-9.

Goodin, Dan. 2017. »Fearing Shadow Brokers leak, NSA reported critical flaw to Microsoft«. *Ars Technica*. 17. Mai 2017. https://arstechnica.com/information-technology/2017/05/fearing-shadow-brokers-leak-nsa-reported-critical-flaw-to-microsoft/ (10.05.2021).

Gordon, John. 2007. »Alice and Bob«. In *Security Protocols*, herausgegeben von Bruce Christianson, Bruno Crispo, James A. Malcolm, und Michael Roe, 344–45. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-540-77156-2_44.

Greenberg, Andy. 2016. »The Father of Online Anonymity Has a Plan to End the Crypto War«. *Wired*, 1. Juni 2016. https://www.wired.com/2016/01/d

avid-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/ (10.05.2021).

Greenwald, Glenn, Ewen MacAskill, und Laura Poitras. 2013. »Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations«. *The Guardian*, 11. Juni 2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (10.05.2021).

Haraway, Donna. 1976. *Crystals, Fabrics, and Fields. Metaphors of Organicism in Twentieth-Century Developmental Biology*. New Haven/London: Yale University Press.

Haraway, Donna. 1991a. »Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective«. In *Simians, Cyborgs, and Women: The Reinvention of Nature*, 183–201. New York: Routledge.

Haraway, Donna. 1991b. »The Biopolitics of Postmodern Bodies: Constitutions of Self in Immune System Discourse«. In *Simians, Cyborgs, and Women: The Reinvention of Nature*, 203–30. New York: Routledge.

Haraway, Donna. 1997. »enlightenment@science_wars.com: A Personal Reflection on Love and War«. *Social Text*

Haraway, Donna. 2018. *Modest_Witness@Second_Millennium. Female-Man©_Meets_OncoMouse™*. Second Edition. New York/London: Routledge.

Heintz, Bettina. 1993. *Die Herrschaft der Regel. Zur Grundlagengeschichte des Computers*. Frankfurt/New York: Campus Verlag.

Helmreich, Stefan. 2000. »Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism«. *Science, Technology, & Human Values* 25 (4): 472–91. https://doi.org/10.1177/016224390002500404.

Hifinger, Rene. 2019. »Drive-by-Downloads und wie Sie sich davor schützen«. *Informationsportal IT-Sicherheit/Ransomware*. 14. Mai 2019. https://www.bundespolizei-virus.de/virenschutz/drive-by-downloads/ (10.05.2021).

Himmelein, Gerald. 1998. »Sicherheitsloch Windows 95/98«. *heise online*, 8. April 1998. https://www.heise.de/newsticker/meldung/Sicherheitsloch-Windows-95-98-13683.html (10.05.2021).

Hocquenghem, Guy. 1993. *Homosexual Desire*. Übersetzt von Daniella Dangoor. Durham/London: Duke University Press.

Hofstadter, Douglas R. 2007. *Gödel, Escher, Bach. Ein Endloses Geflochtenes Band*. München: Klett-Cotta/Deutscher Taschenbuch Verlag.

Höltgen, Stefan, Hg. 2018. *Medientechnisches Wissen, Band 1: Logik, Informationstheorie*. Berlin, Boston: De Gruyter Oldenbourg. https://doi.org/10.1515/9783110477504.

Höltgen, Stefan, Hg. 2019. *Medientechnisches Wissen, Band 2: Informatik, Programmieren, Kybernetik*. Berlin, Boston: De Gruyter Oldenbourg. https://doi.org/10.1515/9783110477504.

Höltgen, Stefan, Hg. 2020. *Medientechnisches Wissen, Band 3: Mathematik, Physik, Chemie*. Berlin, Boston: De Gruyter Oldenbourg. https://doi.org/10.1515/9783110477504.

Hughes, Eric. 1993. »A Cypherpunk's Manifesto«. 1993. https://www.activism.net/cypherpunk/manifesto.html (10.05.2021).

Hutchins, Marcus. 2017. »How to Accidentally Stop a Global Cyber Attacks«. *MalwareTech* (blog). 13. Mai 2017. https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html (10.05.2021).

Joseph L. Popp, Jr. Butterfly Conservatory. o.J. »Joseph L. Popp, Jr. Butterfly Conservatory Official Website«. Zugegriffen 21. September 2017. http://poppbutterflyconservatory.com/Home_Page.html (10.05.2021).

Juhasz, Alexandra, und Theodore Kerr. 2020. »Watching and Talking about AIDS: Analog Tapes, Digital Cultures, and Strategies for Connection«. *First Monday*. https://doi.org/10.5210/fm.v25i10.10283.

Kaczynski, Theodore J. 2010. *Technological Slavery: The Collected Writings of Theodore J. Kaczynski, a.k.a. »The Unabomber«*. Port Townsend, WA: Feral House.

Kahn, David. 1967. *The Codebreakers. The Story of Secret Writing*. New York: The Macmillan Company.

Kaplan, Fred. 2016. »›WarGames‹ and Cybersecurity's Debt to a Hollywood Hack«. *The New York Times*, 19. Februar 2016. https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html (10.05.2021).

Kaspersky. 2019. »46 Prozent mehr Ransomware-Angriffe«. *kaspersky.de*. 27. September 2019. https://www.kaspersky.de/about/press-releases/2019_46-prozent-mehr-ransomware-angriffe (10.05.2021).

Kaspersky. 2020. »Kaspersky Security Bulletin 2020. Statistics«. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf (10.05.2021).

Katz, Jonathan, und Yehuda Lindell. 2008. *Introduction to Modern Cryptography*. Boca Raton/London/New York: Chapman & Hall/CRC.

Keeling, Kara. 2014. »Queer OS«. *Cinema Journal* 53 (2): 152–57.

Kerckhoffs, Auguste. 1883. *La Cryptographie Militaire*. Paris: Librairie Militaire de L. Baudoin et C.

Khomami, Nadia, und Olivia Solon. 2017. »›Accidental Hero‹ Halts Ransomware Attack and Warns: This Is Not Over«. *The Guardian*. 13. Mai 2017.

https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack (10.05.2021).

Kittler, Friedrich. 1986. *Grammophon – Film – Typewriter*. Berlin: Brinkmann & Bose.

Kluge, Friedrich. 2012a. »meta-«. In *Etymologisches Wörterbuch der deutschen Sprache*. Berlin, Boston: De Gruyter. https://www.degruyter.com/document/database/KLUGE/entry/kluge.7250/html (10.05.2021).

Kluge, Friedrich. 2012b. »Metapher«. In *Etymologisches Wörterbuch der deutschen Sprache*. Berlin, Boston: De Gruyter. https://www.degruyter.com/document/database/KLUGE/entry/kluge.7253/html (10.05.2021).

Knight, Peter. 2004. »ILOVEYOU. Viren, Paranoia und die vernetzte Welt«. In *VIRUS! Mutationen einer Metapher*, herausgegeben von Ruth Mayer und Brigitte Weingart, 183–207. Bielefeld: transcript.

Koblitz, Neal, und Alfred J. Menezes. 2007b. »Another Look at ›Provable Security‹«. *Journal of Cryptology* 20 (1): 3–37. https://doi.org/10.1007/s00145-005-0432-z.

Koblitz, Neal, und Alfred Menezes. 2006. »Another Look at ›Provable Security‹ II«. In *Progress in Cryptology – INDOCRYPT 2006*, herausgegeben von Rana Barua und Tanja Lange, 148–75. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/11941378_12.

Koblitz, Neal, und Alfred Menezes. 2007a. »Another Look at Generic Groups«. *Advances in Mathematics of Communications* 1 (1): 13. https://doi.org/10.3934/amc.2007.1.13.

Koblitz, Neal, und Alfred Menezes. 2016. »A Riddle Wrapped in an Enigma«. *IEEE Security Privacy* 14 (6): 34–42. https://doi.org/10.1109/MSP.2016.120.

Koblitz, Neal. 2007. »The Uneasy Relationship Between Mathematics and Cryptography«. *Notices of the AMS* 54 (8): 972–79.

Kocher, Bryan. 1989. »A Hygiene Lesson«. *Communications of the ACM* 32 (1): 3–6.

Kozel, Susan. 2016. »From Openness to Encryption«. *Medium*. 16. Mai 2016. https://medium.com/the-politics-practices-and-poetics-of-openness/from-openness-to-encryption-a57e49917a88 (10.05.2021).

Kozel, Susan. 2017. »Performing encryption«. In *Performing the Digital. Performativity and Performance Studies in Digital Cultures*, herausgegeben von Martina Leeker, Imanuel Schipper, und Timon Beyes, 117–34. Bielefeld: transcript. https://doi.org/10.25969/mediarep/2108.

Krämer, Sybille. 2003. »Erfüllen Medien eine Konstitutionsleistung? Thesen über die Rolle medientheoretischer Erwägungen beim Philosophieren«.

In *Medienphilosophie. Beiträge zur Klärung eines Begriffs*, herausgegeben von Stefan Münker, Alexander Roesler, und Mike Sandbothe, 78–90. Frankfurt a.M.: Fischer Taschenbuch.

Krämer, Sybille. 2008. *Medium, Bote, Übertragung: Kleine Metaphysik der Medialität*. Frankfurt a.M.: Suhrkamp.

Kühl, Eike, und Benjamin Breitegger. 2016. »Der Angriff, der aus dem Kühlschrank kam«. *Zeit Online*, 24. Oktober 2016. https://www.zeit.de/digital/internet/2016-10/ddos-attacke-dyn-internet-der-dinge-us-wahl/komplettansicht (10.05.2021).

Kuhn, Thomas. 1996. *The Structure of Scientific Revolutions*. 3. Aufl. Chicago/London: University of Chicago Press.

Lakoff, George, und Mark Johnson. 1996. *Metaphors We Live By*. Chicago/London: University of Chicago Press.

Landwehr, Dominik. 2008. *Mythos Enigma. Die Chiffriermaschine als Sammler- und Medienobjekt*. Bielefeld: transcript.

Latour, Bruno. 1996. »Ein Türschließer streikt«. In *Der Berliner Schlüssel*, 62–83. Berlin: Akademie Verlag.

Lexico. 2021a. »back door«. In *Lexico*. Oxford University Press. https://www.lexico.com/definition/back_door (10.05.2021).

Lexico. 2021b. »orifice«. In *Lexico*. Oxford University Press. https://www.lexico.com/definition/orifice (10.05.2021).

Little, Keith. 1998. »Almost All The Ways to Find Your Back Orifice«. PC-Help. 1998. https://web.archive.org/web/20050206142157/www.nwinternet.com/~pchelp/bo/morefindBO.htm (10.05.2021).

Little, Keith. 1999. »The Back Orifice ›Backdoor‹ Program. YOUR security is at risk.« PC-Help. 1999. https://www.pc-help.org/www.nwinternet.com/pchelp/bo/bo.html (10.05.2021).

Lloyd, Steve, und Carlisle Adams. 2011. »Key Management«. In *Encyclopedia of Cryptography and Security*, herausgegeben von Henk C. A. van Tilborg und Sushil Jajodia, 683–88. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-5906-5_85.

Loick, Daniel. 2021. »Das Grundgefühl der Ordnung, das alle haben. Für einen queeren Begriff von Sicherheit«. In *Sicherheit. Rassismuskritische und feministische Beiträge*, herausgegeben von Mike Laufenberg und Vanessa E. Thompson, 266–86. Münster: Verlag Westfälisches Dampfboot.

Love, Heather. 2010. »Truth and Consequences: On Paranoid Reading and Reparative Reading«. *Criticism* 52 (2): 235–41. https://doi.org/10.1353/crt.2010.0022.

Lupton, Deborah. 1994. »Panic computing: The viral metaphor and computer technology«. *Cultural Studies* 8 (3): 556–68. https://doi.org/10.1080/09502389400490361.

MacAskill, Ewen. 2018. »I Spy … Another Fiendishly Difficult GCHQ Puzzle Book«. *The Guardian*. 2. August 2018. https://www.theguardian.com/uk-news/2018/aug/03/i-spy-another-fiendishly-difficult-gchq-puzzle-book (10.05.2021).

Mackenzie, Peter. 2019. »WannaCry Aftershock«. *Sophos*. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf (10.05.2021).

Marsh, Sarah. 2017. »NHS Cancer Patients Hit by Treatment Delays after Cyber-Attack«. *The Guardian*, 14. Mai 2017. https://www.theguardian.com/society/2017/may/14/nhs-cancer-patients-treatment-delays-cyber-attack (10.05.2021).

Marston, John. 1820. »The Insatiate Countess«. In *Plays & Poems*, 1–99. London: F. Marshall.

Maurer, Ueli. 2007. »Editor's Note«. *Journal of Cryptology* 20 (1): 1–1. https://doi.org/10.1007/s00145-007-5001-1.

Maurer, Ueli. 2016. »Cryptography and Computation after Turing«. In *The Once and Future Turing*, herausgegeben von S. Barry Cooper und Andrew Hodges, 53–77. Cambridge: Cambridge University Press.

McCann, Hannah, und Whitney Monaghan. 2019. *Queer Theory Now: From Foundations to Futures*. London: Red Globe Press.

McIlwain, Charlton. 2020. »Afrotechtopolis. How Computing Technology Maintains Racial Order«. In *Rethinking Media Research for Changing Societies*, herausgegeben von Matthew Powers und Adrienne Russell, 105–18. Cambridge: Cambridge University Press.

McKinney, Cait, und Dylan Mulvin. 2019. »Bugs: Rethinking the History of Computing«. *Communication, Culture and Critique* 12 (4): 476–98. https://doi.org/10.1093/ccc/tcz039.

McPherson, Tara. 2012. »U.S. Operating Systems at Mid-Century. The Intertwining of Race and UNIX«. In *Race After the Internet*, herausgegeben von Lisa Nakamura und Peter Chow-White, 21–37. New York/London: Routledge.

Menn, Joseph. 2013. »Exclusive: Secret contract tied NSA and security industry pioneer«. *Reuters*, 20. Dezember 2013. http://web.archive.org/web/20131231045803/https://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 (10.05.2021).

Michaelsen, Anja. 2018. »Sedgwick, Butler, Mulvey: Paranoide und reparative Perspektiven in Queer Studies und medienwissenschaftlicher Geschlechterforschung«. In *Kulturwissenschaftliche Perspektiven der Gender Studies*, herausgegeben von Manuela Günter und Annette Keck, 97–116. Berlin: Kadmos.

Microsoft. 2017. »Microsoft Security Bulletin MS17-010 – Critical«. 14. März 2017. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (10.05.2021).

Mrayati, Mohamad, Yahya Meer Alam, und M. Hassan at-Tayyan, Hg. 2003. *al-Kindi's Treatise on Cryptanalysis*. Bd. 1. Series on Arabic Origins of Cryptology. Riyadh: King Faisal Center for Research and Islamic Studies.

mschf.xyz. o.J. »The Persistence Of Chaos«. https://thepersistenceofchaos.com (13.04.2021).

Muhle, Maria. 2008. *Eine Genealogie Der Biopolitik. Zum Begriff Des Lebens Bei Foucault Und Canguilhem*. Bielefeld: transcript.

Muñoz, José Esteban. 2009. *Cruising Utopia. The Then And There Of Queer Futurity*. New York/London: New York University Press.

Munroe, Randall. 2006. »Alice and Bob«. *xkcd*. https://xkcd.com/177/ (10.05.2021).

Munroe, Randall. 2014. »Protocol«. *xkcd*. https://xkcd.com/1323/ (10.05.2021).

Nakashima, Ellen, und Craig Timberg. 2017. »NSA officials worried about the day its potent hacking tool would get loose. Then it did.« *Washington Post*, 16. Mai 2017. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html (10.05.2021).

National Security Agency. 2012. »Computer Network Operations SIGINT Enabling«. *Snowden Surveillance Archive*. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0160/f0ecfcfc.dir/doc.pdf (10.05.2021).

Ney, Peter, Karl Koscher, Lee Organick, Luis Ceze, und Tadayoshi Kohno. 2017. »Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More«. 26th USENIX Security Symposium, 765–79. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/ney (10.05.2021).

o.A. 2013. »Zukunft – Verantwortung – Lernen: Kein Bildungsplan 2015 unter der Ideologie des Regenbogens«. *openPetition*. https://www.openpetition.

de/petition/online/zukunft-verantwortung-lernen-kein-bildungsplan-2015-unter-der-ideologie-des-regenbogens (10.05.2021).

Oberhaus, Daniel. 2018. »›Master/Slave‹ Terminology Was Removed from Python Programming Language«. *Motherboard*, September 2018. https://www.vice.com/en/article/8x7akv/masterslave-terminology-was-removed-from-python-programming-language (10.05.2021).

Ochs, Carsten. 2015. »Die Kontrolle ist tot – lang lebe die Kontrolle! Plädoyer für ein nach-bürgerliches Privatheitsverständnis«. *Mediale Kontrolle unter Beobachtung* 4 (1): 1–35.

Oxford English Dictionary. 1989. »backdoor«. In *Oxford English Dictionary*. Oxford University Press. https://oed.com/oed2/00016298 (10.05.2021).

Oxford English Dictionary. 2011. »Cryptography, n.« In *Oxford English Dictionary*. Oxford University Press. https://www.oed.com/view/Entry/45374 (10.05.2021).

Oxford English Dictionary. 2021. »backdoor«. In *Oxford English Dictionary*. Oxford University Press. https://oed.com/view/Entry/14369? (10.05.2021).

Paar, Christof, und Jan Pelzl. 2016. *Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender*. Berlin/Heidelberg: Springer Vieweg.

Parikka, Jussi. 2005. »The Universal Viral Machine. Bits, Parasites and the Media Ecology of Network Culture«. *ctheory.net*. http://ctheory.net/ctheory_wp/the-universal-viral-machine/ (10.05.2021).

Parikka, Jussi. 2012. *What is Media Archaeology?* Cambridge: Polity Press.

Parikka, Jussi. 2016. *Digital Contagions: A Media Archaeology of Computer Viruses*. 2. Aufl. New York: Peter Lang.

Parthasarathy, Srini. 2012. »Alice and Bob can go on a holiday!« https://drpartha.org.in/publications/alicebob.pdf (10.05.2021).

Perekalin, Alex. 2017. »WannaCry: Are you safe?« *Kaspersky Lab Daily* (blog). 13. Mai 2017. https://www.kaspersky.com/blog/wannacry-ransomware/16518/ (10.05.2021).

Peterson, Andrea. 2013. »Why everyone is left less secure when the NSA doesn't help fix security flaws«. *The Washington Post*, 4. Oktober 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/ (10.05.2021).

Piètre-Cambacédès, Ludovic, und Claude Chaudet. 2010. »The SEMA Referential Framework: Avoiding Ambiguities in the Terms ›Security‹ and ›Safety‹«. *International Journal of Critical Infrastructure Protection* 3 (2): 55–66. https://doi.org/10.1016/j.ijcip.2010.06.003.

Plötz, Andy. 2014. »Queer Politics«. 2014. https://gender-glossar.de/q/item/37-queer-politics (10.05.2021).

Poitras, Laura, und Glenn Greenwald. 2013. »NSA Whistleblower Edward Snowden: ›I Don't Want to Live in a Society That Does These Sort of Things‹ – Video«. *The Guardian*, 9. Juni 2013. https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video (10.05.2021).

Postel, Jon. 1981a. »RFC 790: Assigned Numbers«. 1981. https://tools.ietf.org/html/rfc790 (10.05.2021).

Postel, Jon. 1981b. »RFC 791: Internet Protocol«. 1981. https://tools.ietf.org/html/rfc791 (10.05.2021).

Preciado, Beatriz [Paul B.]. 2003. *Kontrasexuelles Manifest*. Berlin: b_books.

Preciado, Beatriz [Paul B.]. 2015. »Anal Terror. Notes on the First Days of the Sexual Revolution«. *Baedan 3 – journal of queer time travel*, 123–68.

Rehberg, Peter. 2019. »Energie ohne Macht. Christian Maurels Theorie des Anus im Kontext von Guy Hocquenghem und der Geschichte von Queer Theory«. In *Für den Arsch*, 99–139. Berlin: August Verlag.

Rivest, Ron, Adi Shamir, und Len Adleman. 1978. »A Method for Obtaining Digital Signatures and Public-Key Cryptosystems«. *Communications of the ACM* 21 (2): 120–26.

Robert Koch-Institut. 2016. »RKI – Public Health – Das RKI als nationales Public-Health-Institut«. https://www.rki.de/DE/Content/Institut/Public_Health/Beitrag_Jubilaeumsbuch.html (10.05.2021).

Roe, Paul. 2014. »Gender and ›Positive‹ Security«. *International Relations* 28 (1): 116–38. https://doi.org/10.1177/0047117813502503.

Rogaway, Phillip. 2015. »The Moral Character of Cryptographic Work (2015/1162)«. *Cryptology ePrint Archive*, 2015. http://eprint.iacr.org/2015/1162.pdf (10.05.2021).

Ross, Andrew. 1991. »Hacking Away At The Counterculture«. In *Strange Weather: Culture, Science and Technology in the Age of Limits*, 75–100. London/New York: Verso.

Rotman, David. 2020. »We're Not Prepared for the End of Moore's Law«. *MIT Technology Review* (blog). 25. Februar 2020. https://medium.com/mit-technology-review/were-not-prepared-for-the-end-of-moore-s-law-f8798df1835 (10.05.2021).

RSA Conference. 2010. *Bruce Schneier – Who are Alice & Bob?* https://www.youtube.com/watch?v=BuUSi_QvFLY (10.05.2021).

RUB RZ. 2002. »Back Orifice und NetBus«. Rechenzentrum der Ruhr Universität Bochum. https://web.archive.org/web/20050119150947/www.ruhr-uni-bochum.de/sec/bo.htm (10.05.2021).

Salter, Jim. 2020. »OpenZFS Removed Offensive Terminology from Its Code«. *Ars Technica*, Juni 2020. https://arstechnica.com/tech-policy/2020/06/openzfs-removed-master-slave-terminology-from-its-codebase/ (10.05.2021).

Schimpf, Christian-Antonius, Carl-Magnus Ullfors, und Frank Peters. 2001. *Lexikon Computer und Informationstechnik*. Autorisierte Sonderausgabe für Bassermann Verlag. Gütersloh: Bertelsmann.

Schmundt, Hilmar. 2004. »Der Virus und das Virus. Vom programmierten Leben zum lebenden Programm«. In *VIRUS! Mutationen einer Metapher*, herausgegeben von Ruth Mayer und Brigitte Weingart, 159–81. Bielefeld: transcript.

Schneier, Bruce. 1997. »Why Cryptography Is Harder Than It Looks«. *Schneier on Security* (blog). https://www.schneier.com/essays/archives/1997/01/why_cryptography_is.html (10.05.2021).

Schneier, Bruce. 2007. »Did NSA Put a Secret Backdoor in New Encryption Standard?« *Wired*, https://www.wired.com/2007/11/securitymatters-1115/ (10.05.2021).

Schneier, Bruce. 2015. *Applied Cryptography. Protocols, Algorithms, and Source Code in C*. 20th Anniversary Edition. Indianapolis, IN: John Wiley & Sons Inc.

Schneier, Bruce. 2018. *Click here to kill everybody: security and survival in a hyper-connected world*. 1. Aufl. New York: W.W. Norton & Company (E-Book).

Schock, Axel, und Ulli Würdemann. 2017. »So groß die Hoffnung bei dem HIV-Medikament AZT war, so schnell ist sie wieder verflogen«. *magazin.hiv* (blog). 20. März 2017. https://magazin.hiv/2017/03/20/so-gross-die-hoffnung-war-so-schnell-ist-sie-wieder-verflogen/ (10.05.2021).

Schüttpelz, Erhard. 2019. »Methoden sind die Praktiken einer theoretischen Fragestellung«. *Zeitschrift für Medienwissenschaft* 11 (2): 162–64. https://doi.org/10.25969/mediarep/12623.

Sedgwick, Eve Kosofsky. 2003. »Paranoid Reading and Reparative Reading, or, You're So Paranoid, You Probably Think This Essay Is About You«. In *Touching Feeling: Affect, Pedagogy, Performativity*, 123–51. Durham: Duke University Press.

Sevignani, Sebastian. 2012. »The Problem of Privacy in Capitalism and the Alternative Social Networking Site Diaspora*«. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 10 (2): 600–617. https://doi.org/10.31269/triplec.v10i2.394.

Shah, Nadeem, und Mohammed Farik. 2017. »Ransomware – Threats, Vulnerabilities And Recommendations«. *International Journal of Scientific & Technology Research* 6 (6): 307–9.

Shannon, Claude E. 1964. »The Mathematical Theory of Communication«. In *The Mathematical Theory of Communication*, herausgegeben von Claude E. Shannon und Warren Weaver, 10. Aufl., 29–125. Urbana: University of Illinois Press.

Shnayien, Mary. 2014. »Der rosafarbene Elefant im Raum. Überlegungen zur fehlenden Wut über die NSA-Affäre«. *onlinejournal kultur & geschlecht*, Nr. 13 (Juli): 1–18. https://kulturundgeschlecht.blogs.ruhr-uni-bochum.de/wp-content/uploads/2015/08/shnayien_nsa.pdf (10.05.2021).

Shnayien, Mary. 2022. »Sichere Räume, reparative Kritik. Überlegungen zum Arbeiten mit verletzendem Material«. *Zeitschrift für Medienwissenschaft* 14 (1): 54–65. https://doi.org/10.25969/mediarep/18126.

Shostack, Adam. 2014. *Threat Modeling. Designing for Security*. Indianapolis, IN: John Wiley & Sons, Inc.

Shumow, Dan, und Niels Ferguson. 2007. »On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng«. http://rump2007.cr.yp.to/15-shumow.pdf (10.05.2021).

Siegert, Bernhard. 2010. »Türen. Zur Materialität des Symbolischen«. *Zeitschrift für Medien- und Kulturforschung*, 1| 2010: 151–70.

Siegert, Paul Ferdinand. 2008. *Die Geschichte der E-Mail. Erfolg und Krise eines Massenmediums*. Bielefeld: transcript.

Simone, Alina. 2015. »The Strange History of Ransomware«. *Practically Unhackable* (blog). 26. März 2015. https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b (10.05.2021).

Singh, Simon. 2000. *The Code Book: Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor.

Snow, C. P. 2012. *The Two Cultures*. Reissue Edition. Cambridge, U.K.; New York: Cambridge University Press.

Sokal, Alan. 1996a. »A Physicist Experiments With Cultural Studies«. *Lingua Franca*, Nr. May/June: 62–64.

Sokal, Alan. 1996b. »Transgressing the Boundaries: Toward a Transformative Hermeneutics of Quantum Gravity«. *Social Text*, Nr. 46/47: 217–52. https://doi.org/10.2307/466856.

Solomon, Alan, Barry Nielson, und Simon Meldrum. o.J. »AIDS Technical Information [aids.tech.info]«. CERIAS Information Security Archive. http://ftp.cerias.purdue.edu/pub/doc/general/aids.tech.info (10.05.2021).

Solomon, Alan. 1991. *PC Viruses. Detection, Analysis and Cure*. London/Berlin/Heidelberg: Springer.

Spafford, Eugene H. 1989. »The internet worm incident«. In *ESEC '89*, 446–68. Berlin/Heidelberg: Springer. https://doi.org/10.1007/3-540-51635-2_54.

Spafford, Eugene H. 1994. »Computer Viruses as Artificial Life«. *Artificial Life* 1 (3): 249–65. https://doi.org/10.1162/artl.1994.1.3.249.

Spitz, Stephan, Michael Pramateftakis, und Joachim Swoboda. 2011. *Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen*. 2. Aufl. Wiesbaden: Vieweg + Teubner.

Sprenger, Florian, Till A. Heilmann, und Christoph Engemann. 2019. »Wege und Ziele. Die unstete Methodik der Medienwissenschaft«. *Zeitschrift für Medienwissenschaft* 11 (1): 151–61. https://doi.org/10.25969/mediarep/3717.

Sprenger, Florian, Till A. Heilmann, und Christoph Engemann. 2020. »Formatwechsel. Zur Methodendebatte«. *Zeitschrift für Medienwissenschaft* 12 (2): 188–91. https://doi.org/10.25969/mediarep/14826.

Sprenger, Florian, und Christoph Engemann, Hg. 2015b. *Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*. Bielefeld: transcript.

Sprenger, Florian, und Christoph Engemann. 2015a. »Im Netz der Dinge. Zur Einleitung«. In *Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, herausgegeben von Florian Sprenger und Christoph Engemann, 7–58. Bielefeld: transcript.

Sprenger, Florian. 2015. *Politik der Mikroentscheidungen: Edward Snowden, Netzneutralität und die Architekturen des Internets*. Lüneburg: meson press.

Sprenger, Florian. 2016. »TopSecret. Nur für unbefugte Leser«. *Merkur* 70 (801): 85–93.

Sprenger, Florian. 2019. *Epistemologien des Umgebens*. Bielefeld: transcript.

Stauff, Markus. 2005. »Mediengeschichte und Diskursanalyse. Methodologische Variationen und Konfliktlinien«. *Österreichische Zeitschrift für Geschichtswissenschaften* 16 (4): 126–35.

Stengers, Isabelle. 2005. »Introductory Notes on an Ecology of Practices«. *Cultural Studies Review* 11 (1): 183–96. https://doi.org/10.5130/csr.v11i1.3459.

Sullivan, Nick. 2014. »How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer«. *Ars Technica*. https://arstechnica.com/information-technology/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/ (10.05.2021).

Taylor, Paul A. 2001. *Hackers: Crime in the Digital Sublime*. London/New York: Routledge.

The Jargon File. o.J.a. »Alice and Bob«. *The Jargon File*, Version 4.4.7. https://www.catb.org/jargon/html/A/Alice-and-Bob.html (10.05.2021).

The Jargon File. o.J.b. »Back Door«. *The Jargon File*, Version 4.4.7. http://catb.org/jargon/html/B/back-door.html (10.05.2021).

The Jargon File. o.J.c. »SEX«. *The Jargon File*, Version 4.4.7. http://catb.org/~esr/jargon/html/S/SEX.html (10.05.2021).

The Jargon File. o.J.d. »Pubic Directory«. *The Jargon File*, Version 4.4.7. http://catb.org/~esr/jargon/html/P/pubic-directory.html (10.05.2021).

The Jargon File. o.J.e. »RTFM«. *The Jargon File*, Version 4.4.7. https://www.catb.org/jargon/html/R/RTFM.html (10.05.2021).

The Lancet Infectious Diseases. 2020. »The COVID-19 Infodemic«. *The Lancet Infectious Diseases* 20 (8): 875. https://doi.org/10.1016/S1473-3099(20)30565-X.

The No More Ransom Project. o.J.a »The No More Ransom Project«. https://www.nomoreransom.org/index.html (10.05.2021).

The No More Ransom Project. o.J.b »Tipps zur Vorbeugung«. The No More Ransom Project. https://www.nomoreransom.org/de/prevention-advice.html (10.05.2021).

Thieme, Katja, und Mary Ann S. Saunders. 2018. »How do you wish to be cited? Citation practices and a scholarly community of care in trans studies research articles«. *Journal of English for Academic Purposes* 1 (11): 1–11. https://doi.org/10.1016/j.jeap.2018.03.010.

Tholen, Georg Christoph. 2002. *Die Zäsur der Medien: Kulturphilosophische Konturen*. 1. Edition. Frankfurt a.M.: Suhrkamp.

Thomas, Sam L., und Aurélien Francillon. 2018. »Backdoors: Definition, Deniability and Detection«. In *Research in Attacks, Intrusions, and Defenses*, herausgegeben von Michael Bailey, Thorsten Holz, Manolis Stamatogiannakis, und Sotiris Ioannidis. RAID 2018. Lecture Notes in Computer Science, vol. 11050. Cham: Springer.

Treichler, Paula A. 1987. »AIDS, homophobia and biomedical discourse: An epidemic of signification«. *Cultural Studies* 1 (3): 263–305. https://doi.org/10.1080/09502388700490221.

Treichler, Paula A. 1991. »How to Have Theory in an Epidemic: The Evolution of AIDS Treatment Activism«. In *Technoculture*, 57–106. Minnesota, London: University of Minnesota Press.

Turing, Alan. 1987. »Über Berechenbare Zahlen mit einer Anwendung auf das Entscheidungproblem«. In *Alan Turing. Intelligence Service*, herausgegeben

von Bernhard Dotzler und Friedrich Kittler, 17–60. Berlin: Brinkmann & Bose.

Türk, Johannes. 2014. »Zur Begriffsgeschichte der Immunität«. In *Kulturen der Epigenetik. Vererbt, Codiert, Übertragen*, herausgegeben von Vanessa Lux und Jörg Thomas Richter, 107–16. Berlin, Boston: De Gruyter.

Tuschling, Anna. 2020. »Methoden sind politisch«. *Zeitschrift für Medienwissenschaft* 12 (1): 173–78.

Urban Dictionary. o.J. »Backdoor«. *Urban Dictionary*. https://www.urbandictionary.com/define.php?term=Backdoor (10.05.2021).

Vonderau, Patrick. 2019. »Methode als wissenschaftssoziales Problem«. *Zeitschrift für Medienwissenschaft* 11 (2): 165–68. https://doi.org/10.25969/mediarep/12624.

Warnke, Martin. 2011. *Theorien des Internet zur Einführung*. Hamburg: Junius.

Warren, Tom. 2017. »Microsoft issues ›highly unusual‹ Windows XP patch to prevent massive ransomware attack«. *The Verge*, 13. Mai 2017. https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack (10.05.2021).

Watney, Simon. 1996. *Policing Desire. Pornography, AIDS, and the Media*. 3. Edition. Minneapolis: University of Minnesota Press.

Weaver, Warren. 1964. »Recent Contributions to the Mathematical Theory of Communication«. In *The Mathematical Theory of Communication*, herausgegeben von Claude E. Shannon und Warren Weaver, 10. Aufl., 1–28. Urbana: University of Illinois Press.

Webel, Mari. 2020. »Naming the New Coronavirus – Why Taking Wuhan out of the Picture Matters«. *The Conversation*. 18. Februar 2020. http://theconversation.com/naming-the-new-coronavirus-why-taking-wuhan-out-of-the-picture-matters-131738 (10.05.2021).

Weidenbach, Peter, und Johannes vom Dorp. 2020. »Home Router Security Report«. https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf (10.05.2021).

Weingart, Brigitte. 2002. *Ansteckende Wörter. Repräsentationen von AIDS*. Frankfurt a.M.: Suhrkamp.

Whitehead, Alfred North. 1978. *Process and Reality: An Essay in Cosmology*. Gifford Lectures 1927–28. New York: Free Press.

Whittaker, Zack. 2019. »Two Years after WannaCry, a Million Computers Remain at Risk«. *TechCrunch*, 12. Mai 2019. https://social.techcrunch.com/2019/05/12/wannacry-two-years-on/ (10.05.2021).

Wikipedia. 2016. »Microsoft BackOffice Server«. In *Wikipedia*. https://de.wikipedia.org/w/index.php?title=Microsoft_BackOffice_Server&oldid=151543344 (10.05.2021).

Wikipedia. 2017. »Sir Dystic«. In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Sir_Dystic&oldid=817313260 (10.05.2021).

Wilding, Edward. 1990. »Editorial: Joseph Lewis Popp Arrested«. *Virus Bulletin*, März 1990, 2.

Wong, Julia Carrie, und Olivia Solon. 2017. »Massive ransomware cyber-attack hits nearly 100 countries around the world«. *The Guardian*, 12. Mai 2017. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs (10.05.2021).

Young, Adam, und Moti Yung. 1996. »Cryptovirology: extortion-based security threats and countermeasures«. In *Proceedings 1996 IEEE Symposium on Security and Privacy*, 129–40. https://doi.org/10.1109/SECPRI.1996.502676.

Young, Adam, und Moti Yung. 1997. »Kleptography: Using Cryptography Against Cryptography«. In *Advances in Cryptology – EUROCRYPT '97, LNCS 1233*, herausgegeben von Walter Fumy, 62–74. Berlin/Heidelberg: Springer. https://doi.org/10.1007/3-540-69053-0_6.

Young, Adam, und Moti Yung. 2017. »Cryptovirology: The Birth, Neglect, and Explosion of Ransomware«. *Communications of the ACM* 60 (7): 24–26. https://doi.org/10.1145/3097347.

Zarocostas, John. 2020. »How to Fight an Infodemic«. *The Lancet* 395 (10225): 676. https://doi.org/10.1016/S0140-6736(20)30461-X.

Zetter, Kim. 2014. »Hacker Lexicon: What Is an Air Gap?« *Wired*, 12. August 2014. https://www.wired.com/2014/12/hacker-lexicon-air-gap/ (10.05.2021).

Filme

ALIEN. Regie: Ridley Scott. Drehbuch: Dan O'Bannon, Ronald Shusett. UK/USA 1979. 117 Minuten.

BODY SNATCHERS. Regie: Abel Ferrara. Drehbuch: Jack Finney, Raymond Cistheri, Larry Cohen. USA 1993. 87 Minuten.

CITIZENFOUR. Regie: Laura Poitras. UK/DE/USA 2014. 114 Minuten.

INVASION OF THE BODY SNATCHERS. Regie: Don Siegel. Drehbuch: Daniel Mainwaring. USA 1956. 80 Minuten.

Danksagungen

Bei der vorliegenden Publikation handelt es sich um eine unwesentlich überarbeitete Version meiner Dissertationsschrift, die ich im Mai 2021 im Fach Medienwissenschaft an der Fakultät für Philologie der Ruhr-Universität Bochum eingereicht und im darauffolgenden Juli erfolgreich verteidigt habe. Wie jede wissenschaftliche Unternehmung wäre auch diese Arbeit nicht entstanden ohne die zahlreichen Menschen, die mich bei ihrer Herstellung begleitet, ermutigt, versorgt, herausgefordert, aufgefangen und umsorgt haben. Ihnen allen möchte ich an dieser Stelle von Herzen danken.

Mein großer Dank gilt Prof. Dr. Anna Tuschling, die mein Dissertationsprojekt als Erstbetreuerin begleitet und mir den Raum gegeben hat, den ich zum Denken brauchte. Dank ihres stets offenen Ohrs (und Terminkalenders) für meine Fragen und Beobachtungen und ihrer weitsichtigen Einschätzungen sowohl fachlicher Fragen als auch wissenschaftspolitischer Zusammenhänge konnte dieses Dissertationsprojekt in dem herausfordernden Umfeld von *SecHuman* wachsen.

Prof. Dr. Astrid Deuber-Mankowsky, die mein Dissertationsprojekt als Zweitbetreuerin begleitet hat, danke ich sehr für ihre Förderung, Unterstützung und Fürsorge seit Beginn meines Studiums, sowie dafür, dass sie mich immer aufs Neue ins Denken gebracht hat. Ohne ihre klugen Fragen, ihr Attachment, ihre Offenheit und Begeisterung für die Zusammenhänge von Queer Theory, Mathematik und Technik sowie ihr Insistieren auf die Offenheit von Zukünften wäre diese Arbeit nicht ausgekommen.

Prof. Dr. Florian Sprenger danke ich für die Möglichkeit, meine Dissertation ohne Ablenkungen zu ende schreiben zu können. Für die Teilnahme an der Prüfungskommission danke ich neben ihm auch Prof. Dr. Cornelia Wächter.

Den Professor_innen von *SecHuman*, sowie meinen ehemaligen Kolleg_innen danke ich für den Austausch über die Grenzen unserer Disziplinen hinweg, für die produktiven Irritationen, an denen wir gemeinsam gewachsen

sind, und die Aushandlungsprozesse, in denen wir uns situiert haben. Insbesondere danke ich Benedikt Auerbach für seine intellektuelle Großzügigkeit gegenüber Formen der Wissensproduktion, die nicht seine eigenen sind, für die geduldige Erläuterung von Rechenwegen und Formeln, deren Zeichen ich anfangs nicht einmal auszusprechen wusste, für seine Neugier auf medienwissenschaftliche Fragestellungen und für die gründliche Überprüfung dieses Buchs auf seine mathematische Richtigkeit.

Ich hatte das Privileg, Zwischenstände dieses Projekts in verschiedenen Zusammenhängen vorstellen und diskutieren zu dürfen. Mein Dank gebührt Prof. Dr. Penelope Deutscher und den Grad Students der Northwestern University, die für den *Queer Temporalities and Media Aesthetics*-Workshop den Weg nach Bochum gefunden haben, ebenso wie den Mitgliedern der Kolloquien von Prof. Dr. Astrid Deuber-Mankowsky, Prof. Dr. Eva Warth und Prof. Dr. Henriette Gunkel, von Prof. Dr. Stephan Packard und Prof. Dr. Karl-Nikolaus Peifer und von Prof. Dr. Florian Sprenger – sowie selbstverständlich auch den Organisator_innen selbst.

Mein Dank gilt darüber hinaus den vielen wundervollen Kolleg_innen, mit denen ich in den letzten Jahren über meine und ihre Arbeiten sprechen durfte, und die auf ganz unterschiedliche Arten zum Gelingen dieses Projekts beigetragen haben, insbesondere Prof. Dr. Ulrike Bergermann, Jasmin Degeling, Mathias Denecke, Jennifer Eickelmann, Natascha Frankenberg, Naomie Gramlich, Katja Grashöfer, Philipp Hanke, José Herranz Rodriguez, Sarah Horn, Sonja Kirschall, Thomas Nyckel, Felix Raczkowski, Véronique Sina und Uwe Wippich.

Meinen Kolleg_innen am Institut für Medienwissenschaft der RUB, insbesondere Hilde Hoffmann und Eva Hohenberger, danke ich für ihre Herzlichkeit. Susanne von der Heyden dafür, dass ich mit jedem komplizierten Formular zu ihr laufen durfte.

Sonja Kirschall, Jan Nastke, Felix Raczkowski, Carolin Rolf und Noah Simon danke ich für die Filmabende, Spaziergänge und Gin Tonics, die das Leben verschönern. Martin Degeling und bg nerilex danke ich für die langen und großzügigen Diskussionen über technische Details und ihre gesellschaftlichen Zusammenhänge sowie für betreutes Coden.

Jasmin Degeling und Sarah Horn danke ich für das gemeinsame Denken, Schreiben und Sorgen, für ihre Perspektiven und ihren Rückhalt. Len Klapdor danke ich für das unfassbar sorgfältige Korrektorat dieses Manuskripts, das Gefühl von Zu-Hause-Sein und die Wahlverwandtschaft.

Meinem Partner Peter Vignold danke ich dafür, dass er meinen paranoiden Lesarten stets reparative entgegenstellt, für die gemeinsamen Träume und für alles weitere, was ich schlecht in Worte fassen kann.

Meinen Eltern Ani und Rafid Shnayien danke ich für ihre Unterstützung (fast) aller meiner verrückten Ideen, für den guten Zuspruch an den Tagen, an denen ich alles hinschmeißen wollte, und für ihren unerschütterlichen Glauben daran, dass dieses Buch geschrieben werden würde. Alfred Vignold und Jutta Schick danke ich dafür, dass sie uns immer wieder Erholung zwischen den konzentrierten Arbeitsphasen ermöglicht haben.

Der an dieser Stelle letzte Dank gebührt Muise Shnayien und Sona Anasal – ich stehe auf euren Schultern.

Marie-Luise Shnayien ist am Institut für Medienwissenschaft der Ruhr-Universität Bochum assoziierte Postdoc und war zuvor Kollegiatin am interdisziplinären NRW-Forschungskolleg »SecHuman – Sicherheit für Menschen im Cyberspace«. Zu ihren Forschungsschwerpunkten zählen digitale Kulturen und Infrastrukturen, politische Affekte, Mathematikphilosophie sowie die Intersektion von Gender, digitalen Medien und Queer Theory.

Medienwissenschaft

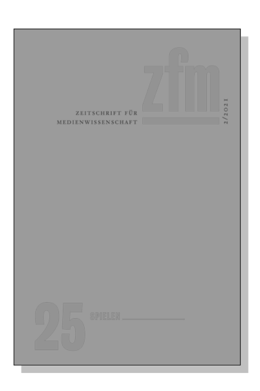


Ziko van Dijk

Wikis und die Wikipedia verstehen

Eine Einführung

2021, 340 S., kart., 13 SW-Abbildungen
35,00 € (DE), 978-3-8376-5645-9
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-5645-3
EPUB: ISBN 978-3-7328-5645-9



Gesellschaft für Medienwissenschaft (Hg.)

Zeitschrift für Medienwissenschaft 25

Jg. 13, Heft 2/2021: Spielen

2021, 180 S., kart.
24,99 € (DE), 978-3-8376-5400-4
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-5400-8
EPUB: ISBN 978-3-7328-5400-4



Anna Dahlgren, Karin Hansson, Ramón Reichert,
Amanda Wasielewski (eds.)

Digital Culture & Society (DCS)

Vol. 6, Issue 2/2020 – The Politics of Metadata

2021, 274 p., pb., ill.
29,99 € (DE), 978-3-8376-4956-7
E-Book:
PDF: 29,99 € (DE), ISBN 978-3-8394-4956-1

Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de